Cat. No. Z919-E1-04

NE2A Series

Safety Network Controller

OPERATION MANUAL

OMRON

NE2A Series
Safety Network Controller

Operation Manual

Revised May 2011

Notice:

OMRON products are manufactured for use according to proper procedures by a qualified operator and only for the purposes described in this manual.

The following conventions are used to indicate and classify precautions in this manual. Always heed the information provided with them. Failure to heed precautions can

result in injury to people or damage to property.

⚠WARNING Indicates a potentially hazardous situation which, if not avoided, will result in minor or moderate injury, or may result in serious injury or death. Additionally, there may be significant property damage.

⚠Caution Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury, or property damage.



Indicates general prohibitions for which there is no specific symbol.



Indicates general mandatory actions for which there is no specific symbol.

OMRON Product References

All OMRON products are capitalized in this manual. The word “Unit” is also capitalized when it refers to an OMRON product, regardless of whether it appears in the proper name of the product.

The abbreviation “PLC” means Programmable Controller. “PC” is used, however, in some Programming Device displays to mean Programmable Controller.

Visual Aids

The following headings appear in the left column of the manual to help you locate different types of information.

IMPORTANT Indicates important information on what to do or not to do to prevent failure to operation, malfunction, or undesirable effects on product performance.

Note Indicates information of particular interest for efficient and convenient operation of the product.

1,2,3... 1. Indicates lists of one sort or another, such as procedures, checklists, etc.

Trademarks and Copyrights

DeviceNet, DeviceNet Safety, EtherNet/IP, and EtherNet/IP Safety are registered trademarks of the Open DeviceNet Vendors Association.

Other product names and company names in this manual are trademarks or registered trademarks of their respective companies.

© OMRON, 2009

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, mechanical, electronic, photocopying, recording, or otherwise, without the prior written permission of OMRON.

No patent liability is assumed with respect to the use of the information contained herein. Moreover, because OMRON is constantly striving to improve its high-quality products, the information contained in this manual is subject to change without notice. Every precaution has been taken in the preparation of this manual. Nevertheless, OMRON assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained in this publication.

TABLE OF CONTENTS

PRECAUTIONS xix

1 Intended Audience xx
2 General Precautions xx
3 Safety Precautions xxii
4 Precautions for Safe Use xxiii
5 Regulations and Standards xxvi
6 Conformance to EC Directives xxvi

SECTION 1
About NE2A-series Safety Network Controllers 1

1-1 Overview 2
1-2 Features 4
1-3 Functions 6
1-4 Preparations for Operation 9

SECTION 2
Configuring a System with NE2A-series Controllers 17

2-1 Devices in the System Configuration 18
2-2 Safety Control System Configuration 21
2-3 Designing Response Performance 26
2-4 Designing Safety Control Logic 27
2-5 Managing Operation 30

SECTION 3
Configuration Unit Specifications and Nomenclature 31

3-1 General Specifications of NE2A-series Controllers 33
3-2 Safety CPU Unit 35
3-3 End Cover 41
3-4 End Unit 42
3-5 Power Supply Unit 43
3-6 DeviceNet Safety Units 46
3-7 EtherNet/IP Safety Units 51
3-8 Safety Input Units 57
3-9 Safety Output Units 62

SECTION 4
Status Transitions and Program Design 67

4-1 NE2A-series Controller Status Transitions 68
4-2 Setting the Operation for Resetting and Starting 73
4-3 Creating Variables 76
4-4 Creating Programs 84

TABLE OF CONTENTS

4-5 Checking Programming 87
4-6 Function Blocks 88

SECTION 5
Communications 91
5-1 Designing the Network System Configuration 92
5-2 Communications Specifications for NE2A-series Controllers 93
5-3 DeviceNet and EtherNet/IP Routing 101
5-4 DeviceNet Safety Communications 102
5-5 DeviceNet Standard Communications 107
5-6 EtherNet/IP Safety Communications 111
5-7 EtherNet/IP Standard Communications 113
5-8 Remote I/O Allocations 121
5-9 Operation after a Communications Error 136
5-10 Selecting the Ethernet Switching Hub 137

SECTION 6
Local I/O Control Functions 139
6-1 NE2A-series Controller Local I/O Specifications 140
6-2 Safety Input Functions 141
6-3 Safety Output Functions 152

SECTION 7
Functions for Operation and Maintenance 157
7-1 Access Control with Passwords 158
7-2 Operation and Maintenance Using a Memory Card 161
7-3 Examples of Security According to Roles 166

SECTION 8
Calculating System Performance 169
8-1 Calculating System Performance 170
8-2 Calculating Safety Response Performance 171
8-3 Calculating Response Performance of Standard Communications 177
8-4 Calculating Cycle Times of NE2A-series Controllers 181
8-5 Calculating Communications Response Performance 183
8-6 Checking and Adjusting the System Response Performance 191

SECTION 9
Basic Network Configurator Operations 193
9-1 Checking before Installation 194
9-2 Installing the Network Configurator 195
9-3 Installing the USB Driver 198

TABLE OF CONTENTS

9-4 Starting and Exiting the Network Configurator 207
9-5 Saving and Reading Network Configuration Files 210
9-6 Main Window and Menus 218

SECTION 10
Designing the System Configuration 231
10-1 NE2A-series Controller Setup 232
10-2 Setting Device Parameters 235

SECTION 11
Setting DeviceNet Networks 239
11-1 DeviceNet Network Setting Procedure 240
11-2 Registering DeviceNet Units to the CPU Unit 241
11-3 DeviceNet Network Settings 245
11-4 Communications between an NE2A-series Controller and a Safety Slave 249
11-5 Using the NE2A-series Controller as a Safety Slave 259
11-6 Communications between the NE2A-series Controller and Standard Slaves 269
11-7 Using an NE2A-series Controller as a Standard Slave 273
11-8 Communications between an NE2A-series Controller and a Standard Master 278

SECTION 12
Setting EtherNet/IP Networks 281
12-1 EtherNet/IP Network Setting Procedure 282
12-2 Registering EtherNet/IP Units to the CPU Unit 283
12-3 EtherNet/IP Network Settings 286
12-4 Communications between an NE2A-series Controller and a Safety Slave 292
12-5 Using the NE2A-series Controller as a Safety Slave 296
12-6 Communications between the NE2A-series Controller and Standard Slaves 297
12-7 Using an NE2A-series Controller as a Standard Slave 298

SECTION 13
Verifying System Performance 307
13-1 System Performance Verification 308
13-2 Checking the NE2A-series Controller Cycle Time 311
13-3 Checking the Communications Response Performance 313
13-4 Verifying the Safety Response Performance (Reaction Time) 327
13-5 Standard I/O Communications Network Response Performance 329

SECTION 14
Setting Parameters for Local I/O 331
14-1 Overall Procedure 332
14-2 Setting the I/O Unit Configuration 333

TABLE OF CONTENTS

14-3 Setting the I/O Configuration from the Wizard 336
14-4 Setting the I/O Configuration of Individual I/O Bits 342

SECTION 15
Creating Programs 351
15-1 Overall Programming Procedure 352
15-2 Starting and Exiting the Logic Editor 353
15-3 Logic Editor Functions 354
15-4 Creating Program Projects 364
15-5 Creating Variables 366
15-6 Creating Programs 376
15-7 Creating Sections 385
15-8 Checking Programs 389
15-9 Creating and Reusing Program Objects 393
15-10 Printing 402

SECTION 16
Mounting, Wiring, and Hardware Settings 407
16-1 Installation Procedure 408
16-2 Wiring 416
16-3 Hardware Settings 422

SECTION 17
Downloading Device Parameters and Operating the Safety Control System 423
17-1 Overall Procedure for Downloading Parameters and Operating the Safety Control System 424
17-2 Connecting Online 425
17-3 Downloading and Uploading Device Parameters 432
17-4 Verifying Parameters and Checking Safety Signatures 439
17-5 Operating the Safety Control System 445
17-6 Protecting Device Parameters 447
17-7 User Test and Automatic Operation 451
17-8 Resetting Devices 454
17-9 Changing Device Parameters and Operating Modes Using a Memory Card 456

SECTION 18
Checking the System Operating Status 463
18-1 Monitoring Programs and Force-setting/resetting Variables 464
18-2 Monitoring Device Status in Maintenance Mode 470
18-3 Monitoring DeviceNet Units 480
18-4 Monitoring EtherNet/IP Units 486

TABLE OF CONTENTS

SECTION 19
Troubleshooting 491

19-1 Checking the Location of an Error 492
19-2 Troubleshooting CPU Unit Errors 494
19-3 Troubleshooting DeviceNet Unit Errors 509
19-4 Troubleshooting EtherNet/IP Unit Errors 522
19-5 Troubleshooting Network Configurator Errors 530
19-6 Connection Status Tables 534

SECTION 20
Inspections and Maintenance 541

20-1 Inspections 542
20-2 NE2A-series Unit Replacement Precautions 543

Appendices 545

Glossary 547

Index 549

Revision History 557

TABLE OF CONTENTS

About this Manual:

This manual describes the installation and operation of the NE2A-series Safety Network Controllers.

Please read this manual carefully and be sure you understand the information provided before attempting to install or operate the NE2A-series Controller. Be sure to read the precautions provided in the following section.

Related Manuals

The following manuals provide information on the DeviceNet and DeviceNet Safety.

NE2A Series Safety Network Controller Operation Manual (Z919)

This manual describes the specifications, functions, and usage of the NE2A-series Safety Network Controllers. (This manual)

NE2A Series Safety Network Controller Command Reference Manual (Z920)

This manual describes the specifications, functions, and usage of instructions for the NE2A-series Safety Network Controllers.

DeviceNet Safety NE0A Series Safety Network Controller Operation Manual (Z916)

This manual describes the specifications, functions, and usage of the NE0A-series Safety Network Controllers.

DeviceNet Safety NE1A Series Safety Network Controller Operation Manual (Z906)

This manual describes the specifications, functions, and usage of the NE1A-series Safety Network Controllers.

DeviceNet Safety System Configuration Manual (Z905-E1-07 or higher)

This manual explains how to configure the DeviceNet Safety system using the Network Configurator.

DeviceNet Safety, Safety I/O Terminal Operation Manual (Z904)

This manual describes the DST1-series Slave models, specifications, functions, and application methods in detail.

EtherNet/IP-DeviceNet Router Operation Manual (Z912)

This manual describes the specifications, functions, and application methods of the EtherNet/IP-DeviceNet Router in detail.

DeviceNet Operation Manual (W267)

This manual describes the construction and connection of a DeviceNet network. It provides detailed information on the installation and specifications of cables, connectors, and other peripheral equipment used in the network, and on the supply of communications power. Obtain this manual and gain a firm understanding of its contents before using a DeviceNet system.

CS/CJ-series DeviceNet Units Operation Manual (W380)

This manual describes the basic settings, Standard Communications, and other aspects of the CS/CJ-series DeviceNet Units.

EtherNet/IP Units Operation Manual (W465)

This manual describes the basic settings, Standard Communications, and other aspects of the CS/CJ-series EtherNet/IP Units.

⚠ **WARNING** Failure to read and understand the information provided in this manual may result in personal injury or death, damage to the product, or product failure. Please read each section in its entirety and be sure you understand the information provided in the section and related sections before attempting any of the procedures or operations given.

Read and Understand this Manual

Please read and understand this manual before using the product. Please consult your OMRON representative if you have any questions or comments.

Warranty and Limitations of Liability

WARRANTY

OMRON's exclusive warranty is that the products are free from defects in materials and workmanship for a period of one year (or other period if specified) from date of sale by OMRON.

OMRON MAKES NO WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, REGARDING NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR PARTICULAR PURPOSE OF THE PRODUCTS. ANY BUYER OR USER ACKNOWLEDGES THAT THE BUYER OR USER ALONE HAS DETERMINED THAT THE PRODUCTS WILL SUITABLY MEET THE REQUIREMENTS OF THEIR INTENDED USE. OMRON DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED.

LIMITATIONS OF LIABILITY

OMRON SHALL NOT BE RESPONSIBLE FOR SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR COMMERCIAL LOSS IN ANY WAY CONNECTED WITH THE PRODUCTS, WHETHER SUCH CLAIM IS BASED ON CONTRACT, WARRANTY, NEGLIGENCE, OR STRICT LIABILITY.

In no event shall the responsibility of OMRON for any act exceed the individual price of the product on which liability is asserted.

IN NO EVENT SHALL OMRON BE RESPONSIBLE FOR WARRANTY, REPAIR, OR OTHER CLAIMS REGARDING THE PRODUCTS UNLESS OMRON'S ANALYSIS CONFIRMS THAT THE PRODUCTS WERE PROPERLY HANDLED, STORED, INSTALLED, AND MAINTAINED AND NOT SUBJECT TO CONTAMINATION, ABUSE, MISUSE, OR INAPPROPRIATE MODIFICATION OR REPAIR.

Application Considerations

SUITABILITY FOR USE

OMRON shall not be responsible for conformity with any standards, codes, or regulations that apply to the combination of products in the customer's application or use of the products.

At the customer's request, OMRON will provide applicable third party certification documents identifying ratings and limitations of use that apply to the products. This information by itself is not sufficient for a complete determination of the suitability of the products in combination with the end product, machine, system, or other application or use.

The following are some examples of applications for which particular attention must be given. This is not intended to be an exhaustive list of all possible uses of the products, nor is it intended to imply that the uses listed may be suitable for the products:

- Outdoor use, uses involving potential chemical contamination or electrical interference, or conditions or uses not described in this manual.
- Nuclear energy control systems, combustion systems, railroad systems, aviation systems, medical equipment, amusement machines, vehicles, safety equipment, and installations subject to separate industry or government regulations.
- Systems, machines, and equipment that could present a risk to life or property.

Please know and observe all prohibitions of use applicable to the products.

NEVER USE THE PRODUCTS FOR AN APPLICATION INVOLVING SERIOUS RISK TO LIFE OR PROPERTY WITHOUT ENSURING THAT THE SYSTEM AS A WHOLE HAS BEEN DESIGNED TO ADDRESS THE RISKS, AND THAT THE OMRON PRODUCTS ARE PROPERLY RATED AND INSTALLED FOR THE INTENDED USE WITHIN THE OVERALL EQUIPMENT OR SYSTEM.

PROGRAMMABLE PRODUCTS

OMRON shall not be responsible for the user's programming of a programmable product, or any consequence thereof.

Disclaimers

CHANGE IN SPECIFICATIONS

Product specifications and accessories may be changed at any time based on improvements and other reasons.

It is our practice to change model numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the products may be changed without any notice. When in doubt, special model numbers may be assigned to fix or establish key specifications for your application on your request. Please consult with your OMRON representative at any time to confirm actual specifications of purchased products.

DIMENSIONS AND WEIGHTS

Dimensions and weights are nominal and are not to be used for manufacturing purposes, even when tolerances are shown.

PERFORMANCE DATA

Performance data given in this manual is provided as a guide for the user in determining suitability and does not constitute a warranty. It may represent the result of OMRON's test conditions, and the users must correlate it to actual application requirements. Actual performance is subject to the OMRON Warranty and Limitations of Liability.

ERRORS AND OMISSIONS

The information in this manual has been carefully checked and is believed to be accurate; however, no responsibility is assumed for clerical, typographical, or proofreading errors, or omissions.

PRECAUTIONS

1 Intended Audience xx
2 General Precautions xx
3 Safety Precautions xxii
4 Precautions for Safe Use xxiii
5 Regulations and Standards xxvi
6 Conformance to EC Directives xxvi
6-1 Applicable Directives xxvi
6-2 Concepts xxvi
6-3 Conformance to EC Directives xxvii

1 Intended Audience

This manual is intended for the following personnel, who must have knowledge of electrical systems (an electrical engineer or the equivalent).

- Personnel in charge of introducing FA and safety systems into production facilities
- Personnel in charge of designing FA and safety systems
- Personnel in charge of managing FA facilities
- Personnel who have the qualifications, authority, and obligation to provide safety during each of the following product phases: mechanical design, installation, operation, maintenance, and disposal

2 General Precautions

The user must operate the product according to the performance specifications described in the operation manuals.

Before using the product under conditions which are not described in the manual or applying the product to nuclear control systems, railroad systems, aviation systems, vehicles, combustion systems, medical equipment, amusement machines, safety equipment, and other systems, machines, and equipment that may have a serious influence on lives and property if used improperly, consult your OMRON representative.

Make sure that the ratings and performance characteristics of the product are sufficient for the systems, machines, and equipment, and be sure to provide the systems, machines, and equipment with double safety mechanisms.

This manual provides information for programming and operating the Unit. Be sure to read this manual before attempting to use the Unit and keep this manual close at hand for reference during operation.

⚠WARNING It is extremely important that a PLC and all PLC Units be used for the specified purpose and under the specified conditions, especially in applications that can directly or indirectly affect human life. You must consult with your OMRON representative before applying a PLC System to the above-mentioned applications

⚠WARNING This is the Operation Manual for the NE2A-series Safety Network Controllers. Heed the following items during system construction to ensure that safety-related components are configured in a manner that allows the system functions to sufficiently operate.

• Risk Assessment

The proper use of the Safety Device described in this Operation Manual as it relates to installation conditions and mechanical performance and functions is a prerequisite for its use. When selecting or using this Safety Device, risk assessment must be conducted with the aim of identifying potential danger factors in equipment or facilities in which the Safety Device is to be applied, during the development stage of the equipment or facilities. Suitable Safety Devices must be selected under the guidance of a sufficient risk assessment system. An insufficient risk assessment system may lead to the selection of unsuitable Safety Devices.

- Typical related international standards: ISO 14121, Safety of Machinery -- Principles of Risk Assessment

- **Safety Measures**

  When using this Safety Device to build systems containing safety-related components for equipment or facilities, the system must be designed with the full understanding of and conformance to international standards, such as those listed below, and/or standards in related industries.

  - Typical related international standards: ISO/DIS 12100, Safety of Machinery -- Basic Concepts and General Principles for Design IEC 61508, Safety Standard for Safety Instrumented Systems (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems)

- **Role of Safety Device**

  This Safety Device is provided with safety functions and mechanisms as stipulated in relevant standards, but suitable designs must be used to allow these functions and mechanisms to operate properly inside system constructions containing safety-related components. Build systems that enable these functions and mechanisms to perform properly, based on a full understanding of their operation.

  - Typical related international standards: ISO 14119, Safety of Machinery -- Interlocking Devices Associated with Guards -- Principles of Design and Selection

- **Installation of Safety Device**

  The construction and installation of systems with safety-related components for equipment or facilities must be performed by technicians who have received suitable training.

  - Typical related international standards: ISO/DIS 12100, Safety of Machinery -- Basic Concepts and General Principles for Design IEC 61508, Safety Standard for Safety Instrumented Systems (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems)

- **Complying with Laws and Regulations**

  This Safety Device conforms to the relevant regulations and standards, but make sure that it is used in compliance with local regulations and standards for the equipment or facilities in which it is applied.

  - Typical related international standards: IEC 60204, Safety of Machinery -- Electrical Equipment of Machines

- **Observing Precautions for Use**

  When putting the selected Safety Device to actual use, heed the specifications and precautions in this Operation Manual and those in the Instruction Manual that comes with the product. Using the product in a manner that deviates from these specifications and precautions will lead to unexpected failures in equipment or devices, and to damages that result from such failures, due to insufficient operating functions in safety-related components.

- **Moving or Transferring Devices or Equipment**

  When moving or transferring devices or equipment, be sure to include this Operation Manual to ensure that the person to whom the device or equipment is being moved or transferred will be able to operate it properly.

  - Typical related international standards: ISO/DIS 12100 ISO, Safety of Machinery -- Basic Concepts and General Principles for Design IEC 61508, Safety Standard for Safety Instrumented Systems (Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems)

3 Safety Precautions

WARNING	
Electric shock may occur. Do not touch any terminals while power is being supplied.	
Serious injury may possibly occur due to loss of required safety functions. Do not use non-safety data as safety signals.	
Serious injury may possibly occur due to loss of required safety functions. Do not use the NE2A-series Controller's test outputs as Safety Outputs.	
Serious injury may possibly occur due to loss of required safety functions. Do not use DeviceNet Standard I/O data, EtherNet/IP Standard I/O data, UDP/IP message data, or explicit message data as safety data.	
Serious injury may possibly occur due to loss of required safety functions. Do not use indicators on the NE2A-series Controller for safety operations.	
Serious injury may possibly occur due to breakdown of Safety Outputs or test outputs. Do not connect loads beyond the rated value to the Safety Outputs and test outputs.	
Serious injury may possibly occur due to loss of required safety functions. Wire the NE2A-series Controller properly so that the 24-VDC line does NOT touch the outputs accidentally or unintentionally.	
Serious injury may possibly occur due to loss of required safety functions. Ground the 0-V line of the power supply for external output devices so that the devices do NOT turn ON when the Safety Output line or the test output line is grounded.	
Serious injury may possibly occur due to loss of required safety functions. Clear previous configuration data before connecting the devices to the network.	
Serious injury may possibly occur due to loss of required safety functions. Set suitable node addresses and a suitable baud rate before connecting the devices to the network.	
Serious injury may possibly occur due to loss of required safety functions. Perform user testing and confirm that all of the device configuration data and operation is correct before starting system operation.	
Serious injury may possibly occur due to loss of required safety functions. When replacing a device, configure the replacement device suitably and confirm that it operate correctly.	
Outputs may operate, possibly resulting in serious injury. Take sufficient safety measures before force-setting or force-resetting variables in the program.	
Serious injury may possibly occur due to loss of required safety functions. Use equipment and parts that comply with applicable standards for the required safety levels and safety categories for all safety functions.	
Serious injury may possibly occur due to loss of required safety functions. Use appropriate components or devices according to the requirements given in the following table.	

Control device	Requirements
Emergency stop switch	Use approved devices with a direct opening mechanism compliant with IEC/EN 60947-5-1.
Door interlocking switch or limit switch	Use approved devices with a direct opening mechanism compliant with IEC/EN 60947-5-1 and capable of switching micro-loads of 4 mA at 24 VDC.
Safety sensor	Use approved devices compliant with the relevant product standards, regulations, and rules in the country where they are used.
Relay with forcibly guided contacts	Use approved devices with forcibly guided contacts compliant with EN 50205. For feedback signals, use devices with contacts capable of switching micro-loads of 4 mA at 24 VDC.
Contactor	Use contactors with a forcibly guided mechanism and monitor the auxiliary NC contact to detect contactor failures. For feedback signals, use devices with contacts capable of switching micro-loads of 4 mA at 24 VDC.
Other devices	Evaluate whether devices used are appropriate to satisfy the requirements of the safety category level.

4 Precautions for Safe Use

■Handling with Care

Do not drop the NE2A-series Controller or subject it to excessive vibration or mechanical shock. The NE2A-series Controller may be damaged and may not function properly.

■Installation and Storage Environment

Do not use or store the NE2A-series Controller in any of the following locations:

- Locations subject to direct sunlight
- Locations subject to temperatures or humidity outside the range specified in the specifications
- Locations subject to condensation as the result of severe changes in temperature
- Locations subject to corrosive or flammable gases
- Locations subject to dust (especially iron dust) or salts
- Locations subject to water, oil, or chemicals
- Locations subject to shock or vibration

Take appropriate and sufficient measures when installing systems in the following locations. Inappropriate and insufficient measures may result in malfunction.

- Locations subject to static electricity or other forms of noise
- Locations subject to strong electromagnetic fields
- Locations subject to possible exposure to radioactivity
- Locations close to power supplies

This is a class A product designed for use in industrial environments. In residential areas it may cause radio interference, in which case the user may be required to take adequate measures to reduce interference.

■Installation and Mounting

- Use the NE2A-series Controller within an enclosure with IP54 protection or higher according to IEC/EN 60529.

- Use DIN Track (TH35-7.5/TH35-15 according to IEC 60715) to install the NE2A-series Controller into the control panel. Mount the NE2A-series Controller to the DIN Track using PFP-M End Plates (not included with the NE2A-series Controller) to prevent it falling off the DIN Track because of vibration. Correctly mount all Units to DIN Track
- Space must be provided around the NE2A-series Controller, at least 20 mm from its side and at least 50 mm from its top and bottom surfaces, for ventilation and wiring.
- Secure the Units, including the Communications Units, End Cover, and Power Supply Unit, with the sliders at the top and bottom of the Units.
- Be sure to lock all locking mechanisms, such as those on I/O Units, I/O terminal blocks, and connectors, before attempting to use the Controller.

Turn the power supply OFF before performing any of the following.

- Connecting or disconnecting Power Supply Units, I/O Units, Communications Units, or any other Units
- Assembling the Controller
- Connecting cables or wiring
- Connecting or removing terminal blocks

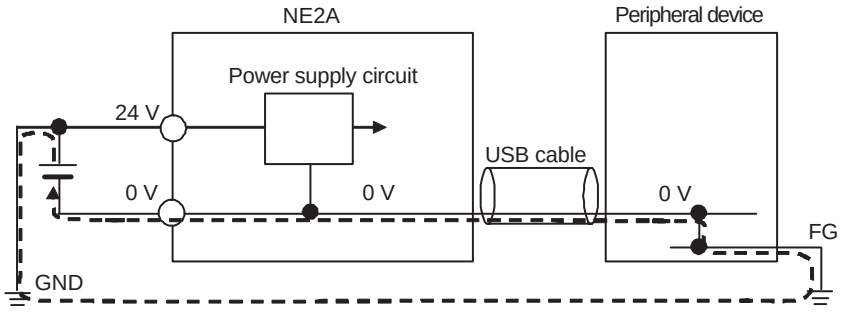
■Installation and Wiring

- Use the following to wire external I/O devices to the NE2A-series Controller.

Solid wire	0.2 to 2.5 mm^2 (AWG 24 to AWG 12)
Stranded wires	0.34 to 1.5 mm^2 (AWG 22 to AWG 16)

- Disconnect the NE2A-series Controller from the power supply before starting wiring. Devices connected to the NE2A-series Controller may operate unexpectedly.
- Properly apply the specified voltage to the NE2A-series Controller inputs. Applying an inappropriate DC voltage or any AC voltage will cause the NE2A-series Controller to fail.
- Be sure to separate the communications cables and I/O cables from near high-voltage/high-current lines.
- Be cautious not to get your fingers caught when attaching connectors to the plugs on the NE2A-series Controller.
- Tighten the power supply terminal block connector screws and DeviceNet connector screws correctly (0.25 to 0.3 N·m).
- Incorrect wiring may lead to loss of safety functions. Wire conductors correctly and verify the operation of the NE2A-series Controller before using the system in which the NE2A-series Controller is incorporated.
- Lock the connectors on Communications Units or I/O Units before using the Units.
- After wiring is completed, be sure to remove label for wire clipping prevention on the NE2A-series Controller to enable heat to escape or proper cooling.

- Do not ground the 24-V side of the power supply to an NE2A-series controller. If you do so, the unwanted current flow shown in the following diagram may occur when you connect a computer or other peripheral device.



■Power Supply Selection

Use a DC power supply satisfying the following requirements.

- The secondary circuits of the DC power supply must be isolated from the primary circuit by double insulation or reinforced insulation.
- The DC power supply must satisfy the requirements for class 2 circuits or limited voltage/current circuits given in UL 508.
- The output hold time must be 20 ms or longer.
- The DC power supply must be an SELV power supply that satisfies the requirements of IEC/EN 60950-1 and EN 50178.

■Periodic Inspections and Maintenance

- Disconnect the NE2A-series Controller from the power supply before replacing the Controller. Devices connected to the NE2A-series Controller may operate unexpectedly.
- Do not disassemble, repair, or modify the NE2A-series Controller. Doing so may lead to loss of safety functions.

■Disposal

- Be cautions not to injure yourself when dismantling the NE2A-series Controller.

5 Regulations and Standards

The following certifications have been obtained for the NE2A-series Safety Network Controller.

Certifying organization	Standards
TÜV Rheinland	EN ISO 13849-1:2008 EN ISO 13849-2:2008 IEC 61508 parts 1-7:1998-2000 IEC 62061:2005 EN 954-1:1996 (ISO 13849-1:1999) IEC 61131-2:2007 EN 60204-1:2006 EN 61000-6-2:2005 EN 61000-6-4:2007 EN ISO 13850:2006 (EN418:1992) NFPA 79-2007 ANSI RIA 15.06-1999 ANSI B11.19-2003
UL	UL 508 UL 1604 Class I, Div. 2, Group A, B, C, D UL 1998 NFPA 79-2002 IEC 61508 CSA 22.2 No.142 CSA 22.2 No.213
Other organizations	CE Marking C-Tick Mark

The NE2A-series Safety Network Controllers can be used to construct safety control network systems that satisfy the following standards.

- SIL 3 (Safety Integrity Level 3) requirements in IEC 61508/IEC 62061
- ISO EN 13849-1 Category 4, PL e

6 Conformance to EC Directives

6-1 Applicable Directives

- EMC Directives

6-2 Concepts

EMC Directives

OMRON devices that comply with EC Directives also conform to the related EMC standards so that they can be more easily built into other devices or the overall machine. The actual products have been checked for conformity to EMC standards (see the following note). Whether the products conform to the standards in the system used by the customer, however, must be checked by the customer.

EMC-related performance of the OMRON devices that comply with EC Directives will vary depending on the configuration, wiring, and other conditions of the equipment or control panel on which the OMRON devices are installed.

The customer must, therefore, perform the final check to confirm that devices and the overall machine conform to EMC standards.

Note Applicable EMC (Electromagnetic Compatibility) standards are as follows:

EMS (Electromagnetic Susceptibility): EN61000-6-2

EMI (Electromagnetic Interference): EN61000-6-4
(Radiated emission: 10-m regulations)

6-3 Conformance to EC Directives

NE2A-series products comply with EC Directives. To ensure that the machine or device in which an NE2A-series product is used complies with EC Directives, the NE2A-series product must be installed as follows:

1,2,3...

1. The NE2A-series product must be installed within a grounded control panel made of metal.
2. The length of the power cable must be no longer than 3 m.
3. The NE2A-series product must be installed within a control panel.
4. The DC power supplies for logic and I/O must meet the following requirements.
   - They must have reinforced insulation or double insulation
   - The output retention time must be 20 ms or longer.
   - They must be SELV power supplies in compliance with IEC/EN 60950-1 and EN 50178.
5. NE2A-series products complying with EC Directives also conform to the Common Emission Standard (EN61000-6-4). Radiated emission characteristics (10-m regulations) may vary depending on the configuration of the control panel used, other devices connected to the control panel, wiring, and other conditions. You must therefore confirm that the overall machine or equipment complies with EC Directives.

SECTION 1
About NE2A-series Safety Network Controllers

This section introduces the NE2A-series Safety Network Controllers.

1-1 Overview 2
1-1-1 About NE2A-series Safety Network Controllers 2
1-1-2 About the Network Configurator 3
1-2 Features 4
1-3 Functions 6
1-4 Preparations for Operation 9
1-4-1 General Steps for Safety Control System Configuration 9
1-4-2 Steps in Building an NE2A-series System 10

1-1 Overview

1-1-1 About NE2A-series Safety Network Controllers

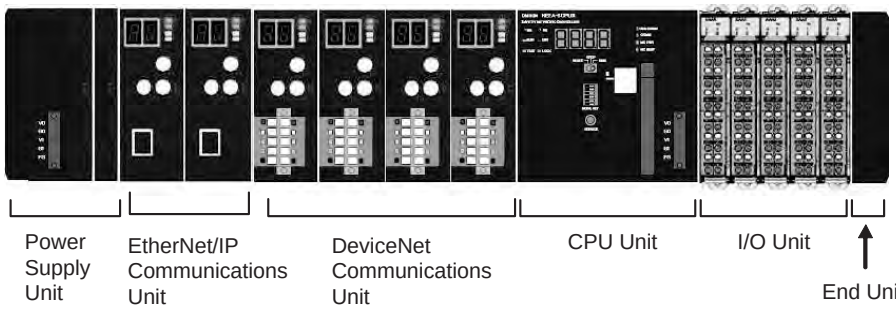
The NE2A-series Safety Network Controllers control Safety Devices such as emergency stop switches and Safety Relays, and support communications using DeviceNet and Ethernet.

Note The NE2A-series Controllers use EtherNet/IP for Ethernet communications. EtherNet/IP supports the CIP (Common Industrial Protocol) on Ethernet.

NE2A-series Controllers can be used to build Safety Control Systems that meet the following requirements.

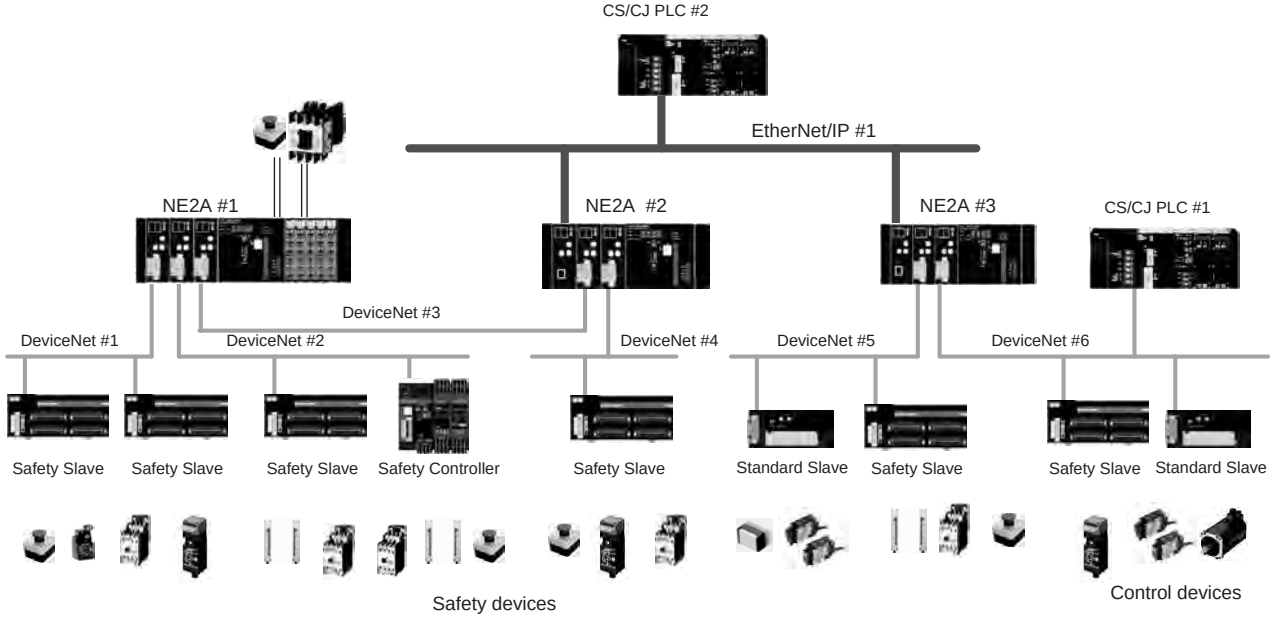
- SIL 3 (Safety Integrity Level 3) requirements in IEC 61508/IEC 62061 (Functional safety of electrical/electronic/programmable electronic safety-related systems)
- ISO EN 13849-1 Category 4, PL e

Appearance of the NE2A-series Controller



System Configuration Using NE2A-series Controllers

As shown in the following system configuration diagram, Safety Control Systems based on NE2A-series Controllers can be used on the same network with device control systems based on Standard PLCs.

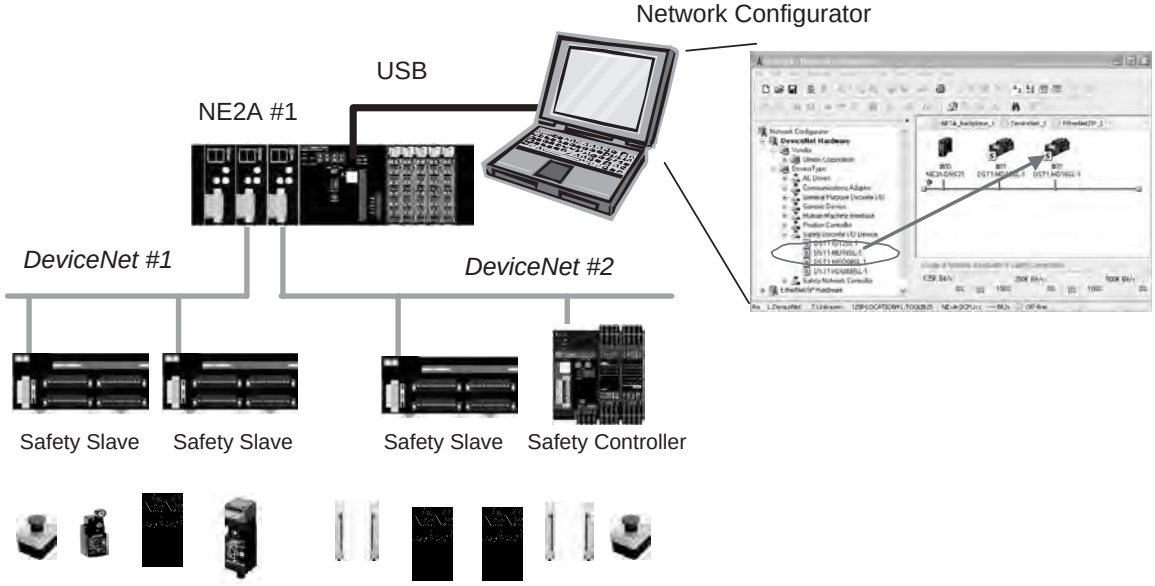


1-1-2 About the Network Configurator

The Network Configurator is a software application for constructing, setting up, and managing DeviceNet and EtherNet/IP networks. In addition, it enables NE2A-series Safety Logic to be easily created using function blocks.

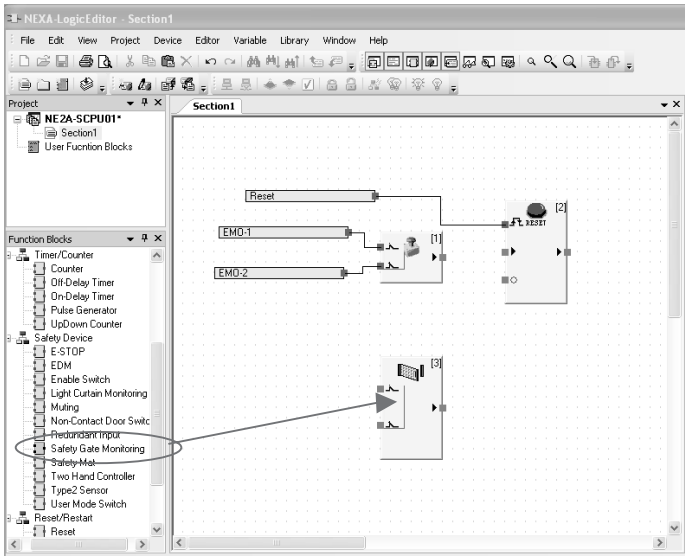
Setting the System Configuration

This example shows the setup for the DeviceNet #1 network for the NE2A #1 Controller. The system configuration can be easily designed by selecting devices and Units from lists.



Logic Design

The design of logic (programming) for NE2A-series Controllers is created using function blocks. Logic can be easily designed by selecting function blocks from lists.



1-2 Features

Applicable to Large-scale Systems

- NE2A-series Controllers support EtherNet/IP Safety Communications, EtherNet/IP Standard Communications, DeviceNet Safety Communications, and DeviceNet Standard Communications.
- A total of up to six EtherNet/IP Units and DeviceNet Units can be mounted in each NE2A-series Controller, making it possible to build large-scale Safety Control Systems. Up to three EtherNet/IP Units and up to six DeviceNet Units can be mounted to each PLC.
- A total of 160 connections per CPU Unit are supported for an EtherNet/IP Safety Master or DeviceNet Safety Master.

  System Configuration Example:

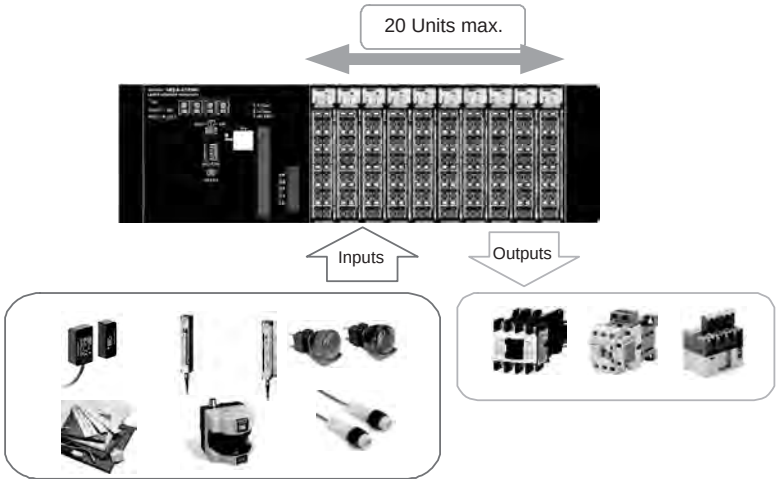
  When a Safety Network is configured with DeviceNet as described below, a system can be constructed with 480 Safety Inputs and 480 Safety Outputs.

  ➢ Mount 6 DeviceNet Safety Units in an NE2A-series Controller.

  ➢ Connect 10, DST1-MD16SL-1 Safety I/O Terminals (with 8 Safety Inputs and 8 Safety Outputs each) in each DeviceNet network.
- Configuration information can be downloaded and uploaded, and the devices can be monitored online across the networks.

Enhanced Expandability

- NE2A-series Communications Units and local I/O can be expanded in building-block fashion.
- EtherNet/IP and DeviceNet Communications Units can be freely used in combination in constructing a system.
- The number of local I/O points can be expanded by adding I/O Units (4 Safety Inputs or 4 Safety Outputs each) to build a system with the optimum number of I/O points.



Greater Integration of Safety Device Connections

- Safety Mats, D40A Non-contact Door Switches, and Single-beam Safety Sensors can be directly connected to NE2A-series Safety Input Units. Being able to connect directly without connecting through special controllers makes it possible to reduce costs and to save space in the control panel.

Design Environment for Easier Programming

- A wide selection of safety-related function blocks enables more efficient program development.
- Program files and user-defined function blocks created using NE2A-series Controllers can be reused as program components.
- Programs and user-defined function blocks created using NE1A-series Controllers can also be used, enabling effective use of existing resources.

Complete System Startup Support

- The Logic Editor can simultaneously display and monitor multiple programs. With online monitoring, errors that occur at devices on the network can be easily identified on the Network Configurator monitor screen.
- The variables used in the program can be force-set or force-reset, regardless of the ON/OFF status of local I/O and remote I/O. This makes it possible to debug programs during system installation before all local I/O and remote I/O are connected. In addition, output wiring can be efficiently checked.

Improved Maintenance Efficiency

- When an error occurs, the Network Configurator can be connected and the communications node where the error occurred can be isolated and stopped for troubleshooting.
- The cause of stopping operation can be immediately determined on the 7-segment display on the Controller and in the error log and operation history at the Configurator.
- A Memory Card can be used to download parameters and the operating mode can be changed. This makes it easy to replace or repair communications nodes without having to use the Network Configurator. Parameters can be downloaded not only to individual CPU Units, but also to all of the nodes on the DeviceNet network to which a CPU Unit is connected.

Access Control by Passwords

- The network configuration and programming information is protected by passwords set for the NE2A-series Controller.
- Access to network configuration files and program files created by the Network Configurator is also password controlled.

1-3 Functions

Function	Summary	Reference
Communications Control Functions		
DeviceNet Safety Communications	The Controller provides the functions of a DeviceNet Safety Master and a DeviceNet Safety Slave. It can communicate with devices that support DeviceNet Safety.	5-4
EtherNet/IP Safety Communications	The Controller provides the functions of an EtherNet/IP Safety Master and an EtherNet/IP Safety Slave. It can communicate with devices that support EtherNet/IP Safety. The wide network bandwidth enables construction of large-scale systems.	5-6
DeviceNet Standard Communications	The Controller provides the functions of a DeviceNet Standard Master and a DeviceNet Standard Slave. It can communicate with devices that support DeviceNet. Systems can be constructed for operations such as coordinating with Standard Controllers and monitoring Safety Controls.	5-5
EtherNet/IP Tag Data Links	The Controller has a Tag Data Link Target function so that it can communicate with Originator devices (Controllers) that support EtherNet/IP Tag Data Links. Systems can be constructed for operations such as coordinating with Standard Controllers and monitoring Safety Controls.	5-7
Assembly definitions	Defining the I/O data used for communications by DeviceNet and EtherNet/IP enables the intended data to be sent and received with no need for special programming.	5-8
Communications stop/continue when a safety communications error occurs	I/O communications operations at the connection where the error occurs can be set to stop or continue when a communications error (connection timeout) occurs during Safety I/O Communications with a Safety Slave. That connection can be restored (or replaced) without having to stop the entire system.	5-9
Explicit message communications	NE2A-series Controller status information can be read by using the explicit message service.	
I/O Control Functions		
Building-block local I/O	Local I/O is configured from building-block I/O Units. The number of I/O points can be increased by adding I/O Units. This makes it possible to build a system with the optimum number of I/O points. An individual Unit can be replaced without removing the base block from the DIN Track or changing the wiring.	SECTION 6 16-1
Safety Input device diagnosis	The following errors can be detected by diagnosis of input circuits and of externally connected devices using test pulses from output terminals: Input circuit errors, externally connected device errors (input terminal test pulse errors), test output terminal overcurrent detection, and test output terminal output ON errors.	6-2
Safety Output device diagnosis	The Controller has Safety Output functions. The following errors are detected by the overcurrent detection function and the short-circuit detection function based on test pulse outputs when outputs turn ON: Overcurrent detection, short-circuit detection, output errors (short-circuiting with 24 V or between output terminals).	6-3
Dual channel evaluation	If an error occurs on one side between two related local inputs or two local outputs, the two inputs or two outputs will go into the safe state without depending on the user program.	6-2 6-3
Input ON delay and OFF delay	Influence from chattering and external noise can be reduced by setting the input time constant for inputs to 0, 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, or 1,024 ms.	6-2

Function	Summary	Reference
Safety Logic Programming		
Programming with variables	Variables are used to assign I/O, status, and other data to variables for use in programming. It enables programming without any need to pay attention to local I/O allocations or to remote I/O connection settings and allocations. Once a program has been created, it does not have to be changed when the system configuration is changed. Programming with variables also improves program reusability.	SECTION 4
Naming	Networks and NE2A-series CPU Units can be named, and names can also be given to each I/O terminal on I/O Units. These names can then be displayed in the I/O list in the Program Editor.	
Programming with function blocks	Function blocks are supported, such as logic functions (AND, OR, etc.), emergency stop pushbutton monitoring, and safety door monitoring.	4-4
User-defined function blocks	New function blocks can be defined by combining function blocks supplied for the NE2A-series Controller.	4-4
Library management of program components	The Controller has a function that lets you manage program components as library objects. Designing can be made more efficient by reusing program components from the library.	4-4
User program ID	Any 4-digit number can be registered as the ID of a user program. Then the program can be known by displaying the registered ID on the 7-segment display.	
Program Execution and Testing		
Monitoring variables (Watch Window)	Multiple variables in a program can be monitored at the same time.	18-1
Force-setting/resetting variables	Input signals to and output signals from the user program can be set (turned ON) or reset (turned OFF) regardless of the status of external input devices or the results of user program execution.	4-1
Cycle time calculation	The instruction execution cycle time and peripheral servicing cycle time are automatically calculated by the Network Configurator according to the configuration, such as the size of the program, the number of I/O Units, the number of Communications Units, and the connection settings.	8-2
Program execution start delay	This function delays program execution until Safety I/O Communications are started. A logic error may occur at the function block if the program is executed without waiting for the start of Safety I/O Communications. Logic errors can be prevented by using this function.	4-1
Security		
Project file protection	Passwords can be set for project files to prevent unexpected changes. These passwords are called project file passwords.	7-1, 7-3
Parameter protection	Passwords can be set to restrict access to NE2A-series Controller parameters (including programs) to prevent unexpected references and changes. These passwords are called parameter passwords.	7-1, 7-3
Device protection	Passwords can be set for devices to prevent unexpected parameter and program downloading or to prevent changes to operating status. These passwords are called device passwords.	7-1, 7-3
User-defined function block protection	Passwords can be set to restrict access to user-defined function blocks to prevent unintentional access and changes to user-defined function blocks. These passwords are called used-defined function block passwords.	7-1, 7-3
Monitoring from the Network Configurator		
Online monitoring	Controller status information and I/O data can be monitored online using the Network Configurator.	18-1
Device status monitoring	Status held in the Controller can be monitored.	18-2
Local I/O status monitoring	The local I/O status of the Controller can be monitored.	18-2-6
Maintenance parameters status monitoring	The present values of Controller maintenance parameters can be monitored.	18-2

Function	Summary	Reference
CIP Safety Connection status monitoring	CIP Safety Connection status can be monitored. If an error occurs in establishing a connection, the error code will be displayed and a help screen can be opened to show the details of the error. That error status will also be displayed when a Safety I/O Communications timeout error occurs.	18-2
CIP Standard Connection status monitoring	DeviceNet connection status and EtherNet/IP Tag Data Link connection status can be monitored. If an error occurs in establishing a connection, the error code will be displayed and a help screen can be opened to show the details of the error. That error status will also be displayed when a Safety I/O Communications timeout error occurs.	18-2
Operation history and error log monitoring	The history of operations executed by the Controller and the history of errors detected by the Controller are saved separately. These histories can be monitored, cleared, and saved in a personal computer.	18-3, 18-4
Maintenance		
Downloading by using a Memory Card	The configuration can be downloaded to the Controller or to the Controller and the devices on the same DeviceNet network, without requiring a personal computer.	7-2
Locking by using a Memory Card	The configuration can be locked for the Controller or for the Controller and the devices on the same DeviceNet network, without requiring a personal computer.	7-2
Operation checking with RUN/STOP/RESTART switch	The RUN/STOP/RESTART switch can be used to start and stop program execution and to restart the Controller, enabling operations to be checked onsite without requiring a personal computer.	7-2
Total run time management	The Controller accumulates and records the time from when the power supply is turned ON.	18-2
Number of contact operations	With each local input or local output contact, the OFF to ON count is incremented and saved internally. If the total count reaches a threshold value, the applicable Connected Device Maintenance Flag in the connected device maintenance status turns ON.	18-2

1-4 Preparations for Operation

1-4-1 General Steps for Safety Control System Configuration

When using the NE2A-series Controller to construct a system of safety-related components for the applicable equipment and devices, design the system in conformance with international standards and the related industrial standards, such as ISO 12100-1, IEC 61508, and IEC 62061.

For example, as shown below, ISO 12100-1 requires measures for reducing risk by determining the level of danger of the machinery and then following safety design procedures.

Step 1: Determine the operating range of the machine.

Step 2: Identify the hazards and assess the risks.

Step 3: Remove hazards and reduce risks as much as possible through a basic safety design.

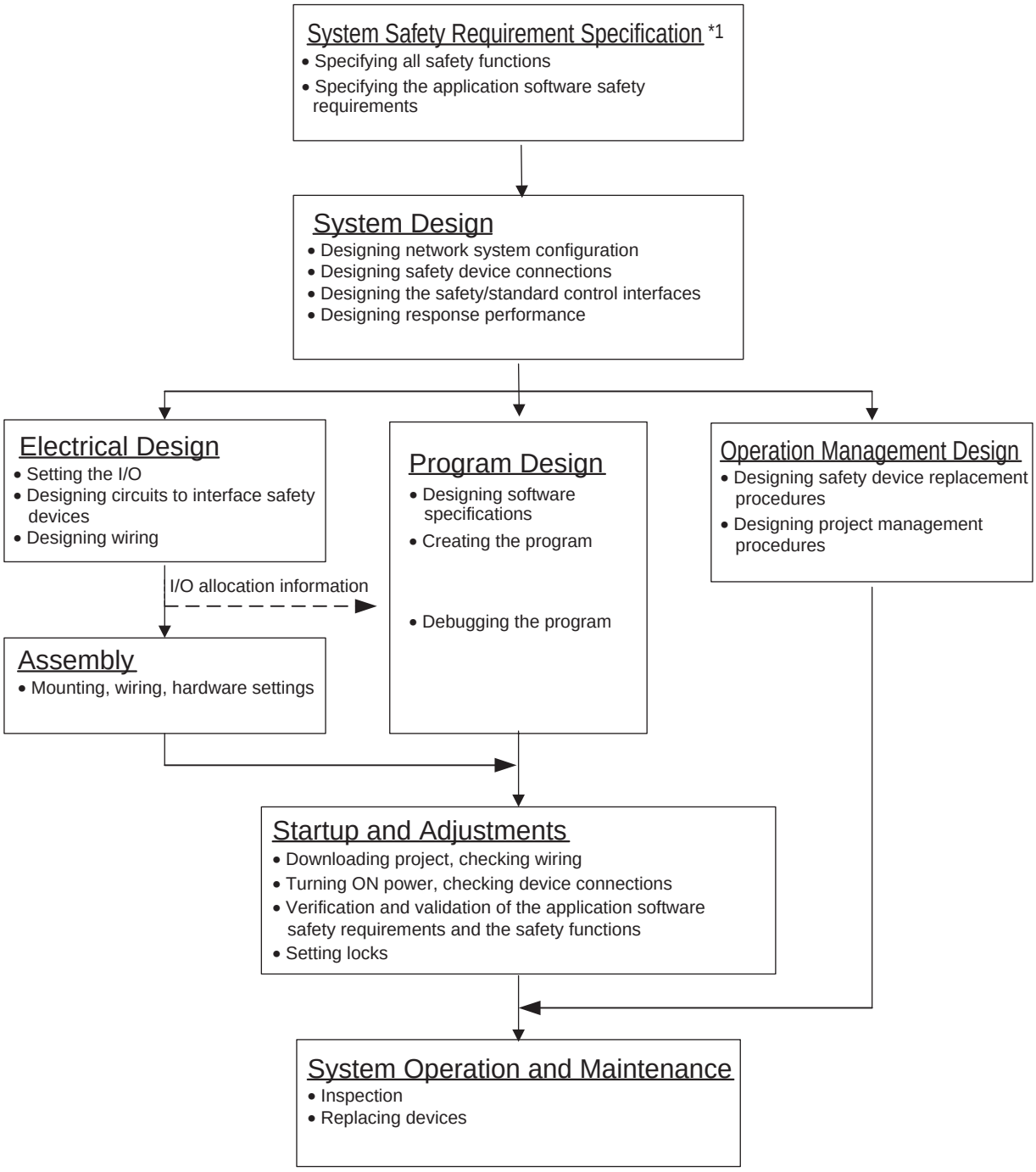
Step 4: Design guards, safety equipment, and other safeguards against any residual risks.

Step 5: Inform and warn users about any residual risks.

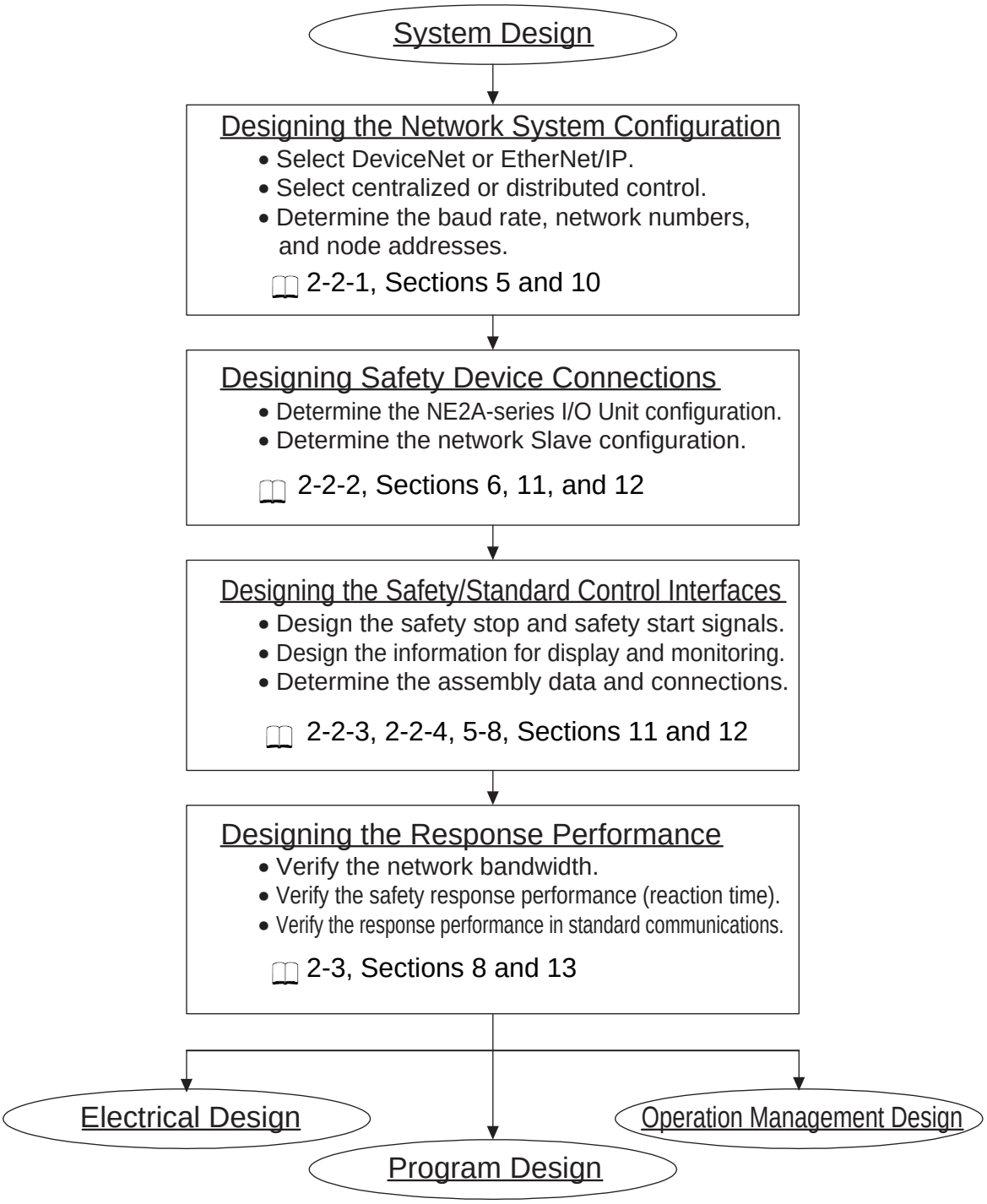
1-4-2 Steps in Building an NE2A-series System

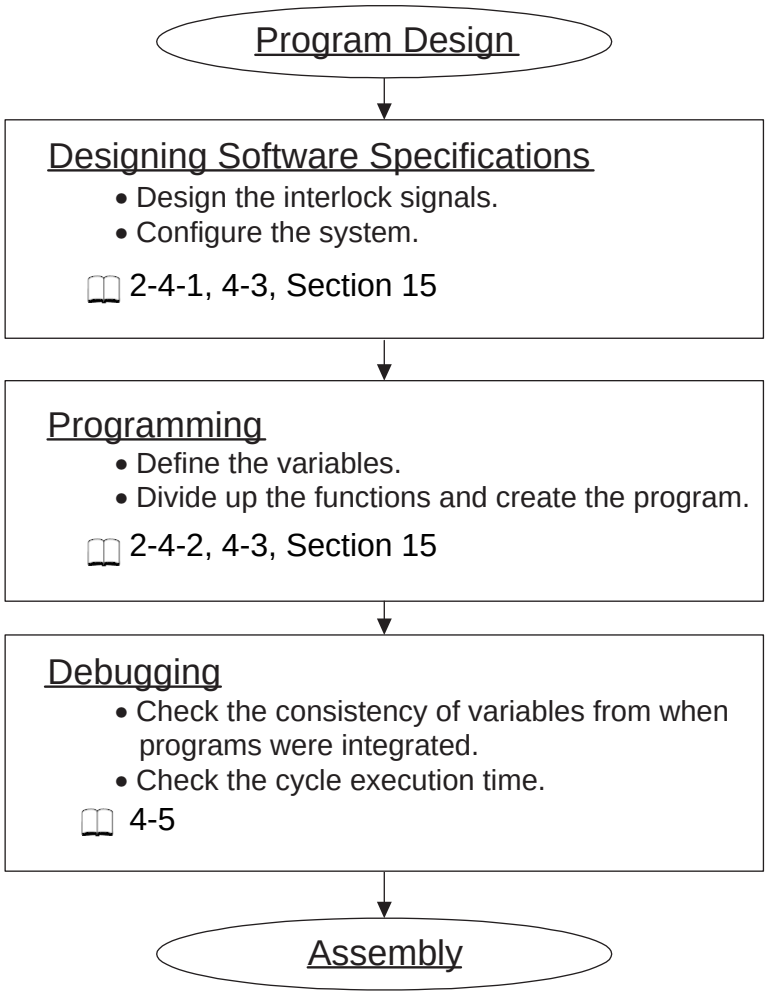
The general procedure is shown below.

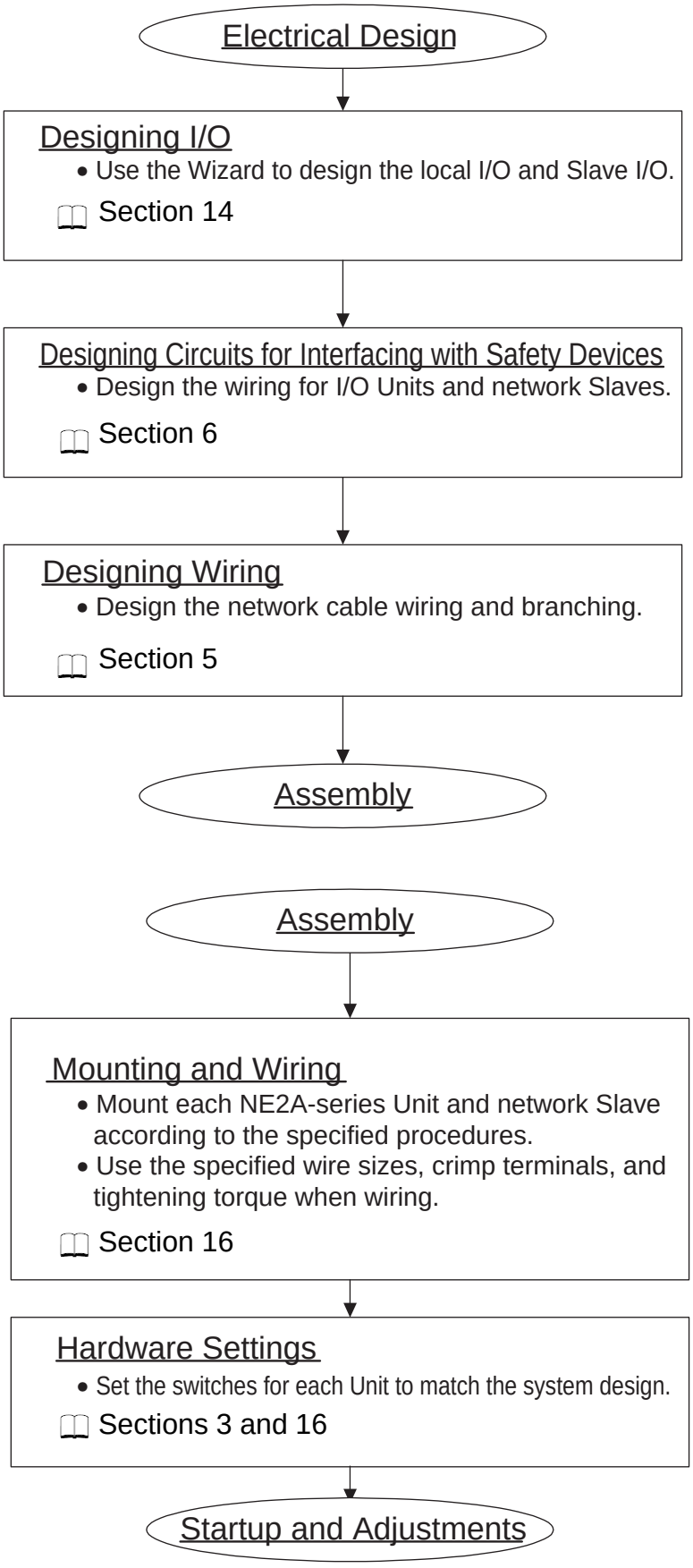
The contents of each step are described in the subsequent sections. Detailed descriptions are provided in the reference locations.

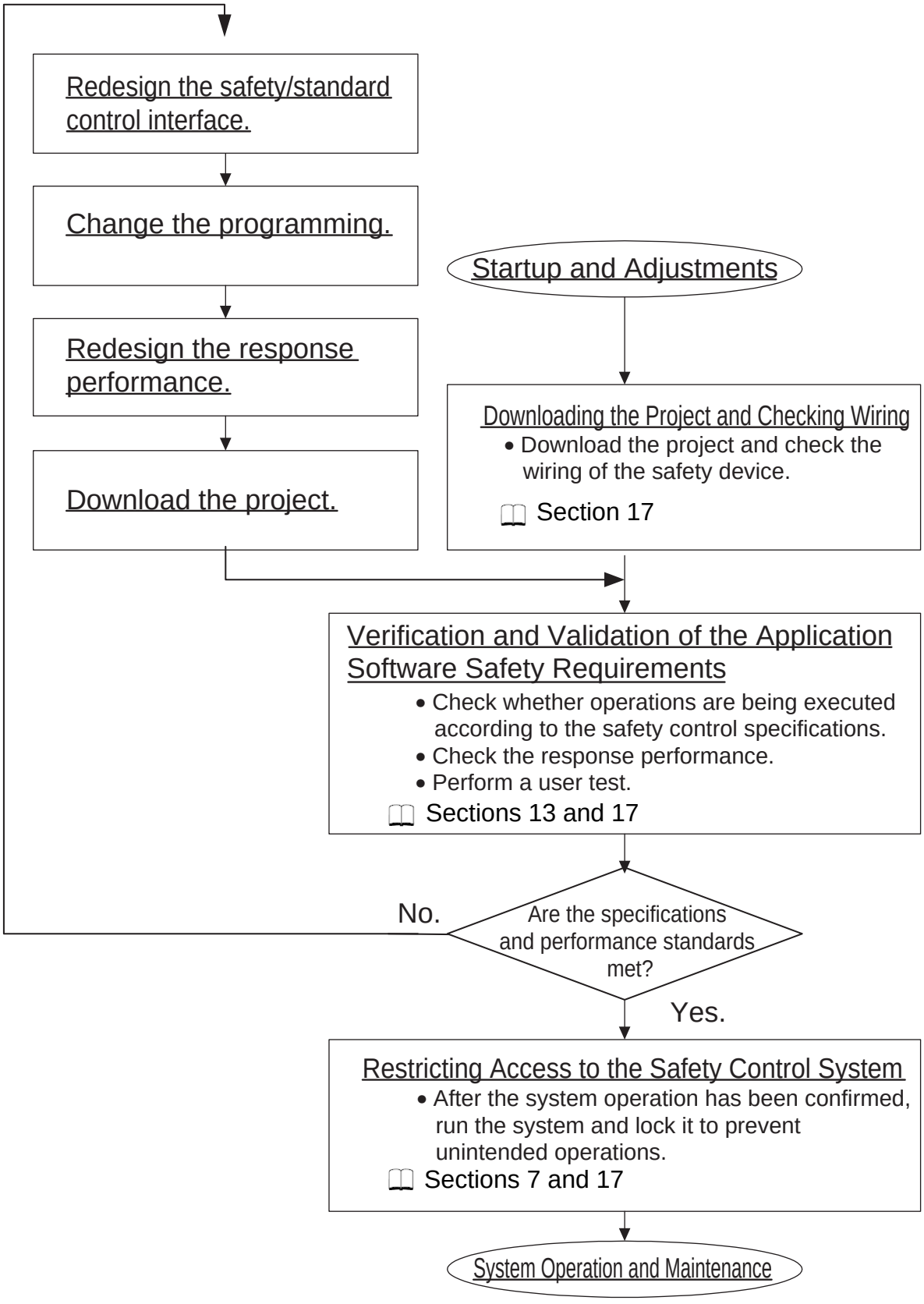


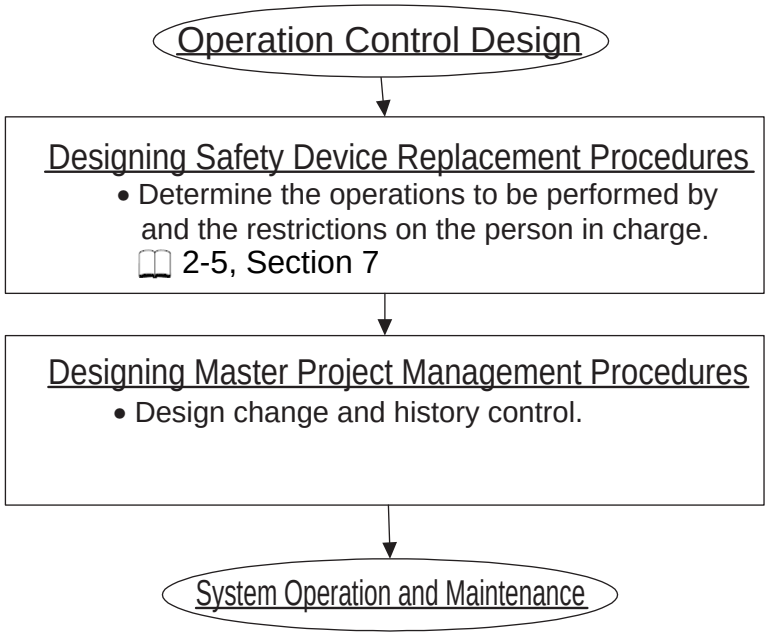
*1 This step determines the safety requirements of the overall system. This information is beyond the scope of this manual and has therefore been omitted.

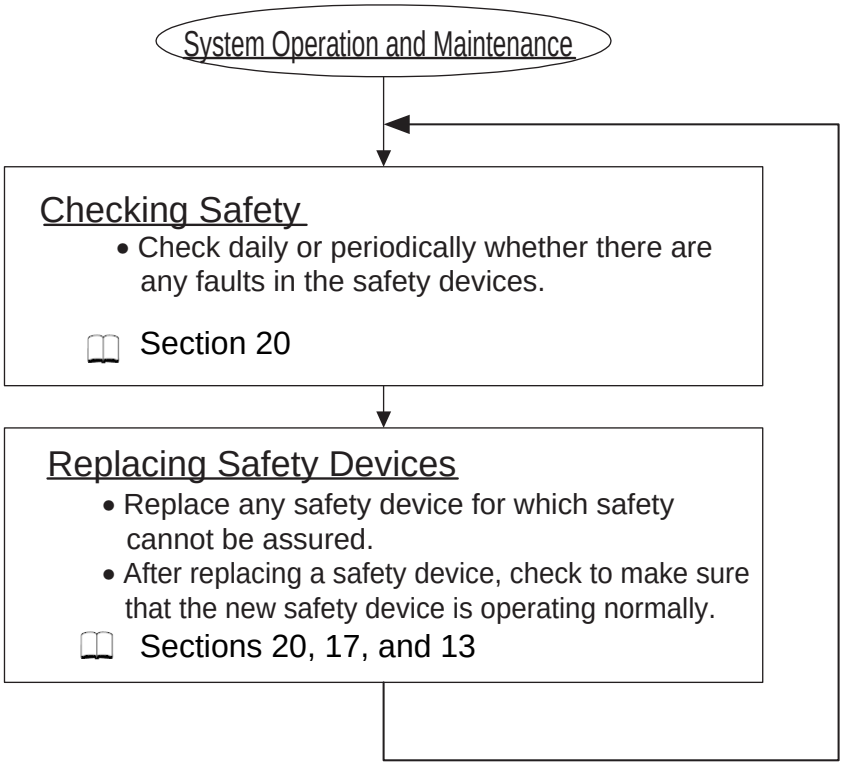

System Design
Designing the Network System Configuration
• Select DeviceNet or EtherNet/IP.
• Select centralized or distributed control.
• Determine the baud rate, network numbers, and node addresses.
2-2-1, Sections 5 and 10
Designing Safety Device Connections
• Determine the NE2A-series I/O Unit configuration.
• Determine the network Slave configuration.
2-2-2, Sections 6, 11, and 12
Designing the Safety/Standard Control Interfaces
• Design the safety stop and safety start signals.
• Design the information for display and monitoring.
• Determine the assembly data and connections.
2-2-3, 2-2-4, 5-8, Sections 11 and 12
Designing the Response Performance
• Verify the network bandwidth.
• Verify the safety response performance (reaction time).
• Verify the response performance in standard communications.
2-3, Sections 8 and 13
Electrical Design
Program Design
Operation Management Design


Program Design
Designing Software Specifications
• Design the interlock signals.
• Configure the system.
2-4-1, 4-3, Section 15
Programming
• Define the variables.
• Divide up the functions and create the program.
2-4-2, 4-3, Section 15
Debugging
• Check the consistency of variables from when programs were integrated.
• Check the cycle execution time.
4-5
Assembly


Electrical Design
Designing I/O
• Use the Wizard to design the local I/O and Slave I/O.
Section 14
Designing Circuits for Interfacing with Safety Devices
• Design the wiring for I/O Units and network Slaves.
Section 6
Designing Wiring
• Design the network cable wiring and branching.
Section 5
Assembly
Assembly
Mounting and Wiring
• Mount each NE2A-series Unit and network Slave according to the specified procedures.
• Use the specified wire sizes, crimp terminals, and tightening torque when wiring.
Section 16
Hardware Settings
• Set the switches for each Unit to match the system design.
Sections 3 and 16
Startup and Adjustments


Redesign the safety/standard control interface.
Change the programming.
Redesign the response performance.
Download the project.
Startup and Adjustments
Downloading the Project and Checking Wiring
• Download the project and check the wiring of the safety device.
Section 17
Verification and Validation of the Application Software Safety Requirements
• Check whether operations are being executed according to the safety control specifications.
• Check the response performance.
• Perform a user test.
Sections 13 and 17
Are the specifications and performance standards met?
No.
Yes.
Restricting Access to the Safety Control System
• After the system operation has been confirmed, run the system and lock it to prevent unintended operations.
Sections 7 and 17
System Operation and Maintenance


Operation Control Design
Designing Safety Device Replacement Procedures
• Determine the operations to be performed by and the restrictions on the person in charge.
2-5, Section 7
Designing Master Project Management Procedures
• Design change and history control.
System Operation and Maintenance


System Operation and Maintenance
Checking Safety
• Check daily or periodically whether there are any faults in the safety devices.
Section 20
Replacing Safety Devices
• Replace any safety device for which safety cannot be assured.
• After replacing a safety device, check to make sure that the new safety device is operating normally.
Sections 20, 17, and 13

SECTION 2
Configuring a System with NE2A-series Controllers

This section describes how to configure a system using NE2A-series Safety Network Controllers, including designing performance and control logic.

2-1 Devices in the System Configuration 18
2-2 Safety Control System Configuration 21
2-2-1 Network System Configuration 21
2-2-2 Connecting Safety Devices 23
2-2-3 Designing a Safety Control Interface 24
2-2-4 Designing a Standard Control Interface 24
2-3 Designing Response Performance 26
2-3-1 Verifying the Network Bandwidth 26
2-3-2 Verifying Safety Response Performance (Reaction Times) 26
2-3-3 Verifying Response Performance in Standard Communications . . . 26
2-4 Designing Safety Control Logic 27
2-4-1 Designing the Program 27
2-4-2 Programming with Variables 28
2-5 Managing Operation 30
2-5-1 Restricting Access to Safety Control Systems 30
2-5-2 Using Memory Cards to Download and Lock Parameters 30

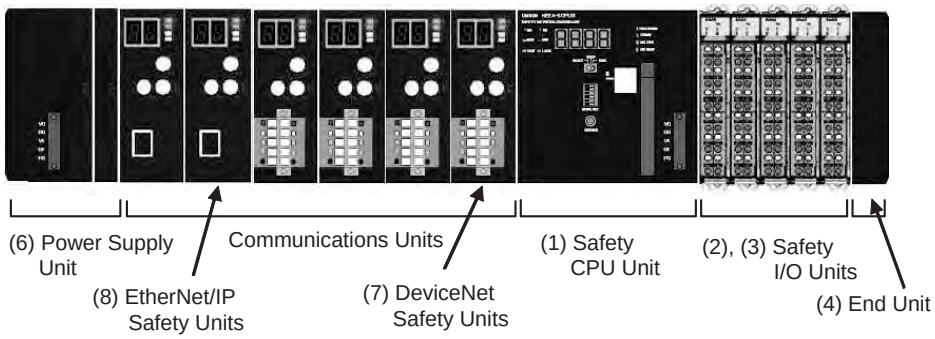
2-1 Devices in the System Configuration

The following table lists the devices used in a Safety Control System configured with an NE2A-series Controller.

Series name, product name, model number		Description
NE2A Series	Safety CPU Unit NE2A-SCPU01 . . . . . (1)	The NE2A-SCPU01 Safety CPU Unit is the part of the Safety Controller that controls safety according to a Safety Program. It provides interfaces for Safety I/O Units and Communications Units so it can be used to build the optimum system configuration.
	Safety Input Unit NE2A-SID4-1 . . . . . (2)	The NE2A-SID4-1 is a building-block Safety Input Unit that can be mounted to the NE2A-series Controller and used as local I/O.
	Safety Output Unit NE2A-SOD4-1 . . . . . (3)	The NE2A-SOD4-1 is a building-block Safety Output Unit that can be mounted to the NE2A-series Controller and used as local I/O.
	End Unit NE2A-END . . . . . (4)	The NE2A-END End Unit is mounted to the right of the NE2A-series CPU Unit or a Safety I/O Unit. It is required even when Safety I/O Units are not used. The End Unit is included with the CPU Unit.
	End Cover NE2A-TER01 . . . . . (5)	The NE2A-TER01 End Cover is mounted to the left of the NE2A-series CPU Unit or Communications Unit. It is not required when the system includes a Power Supply Unit. The End Cover is included with the CPU Unit.
	Power Supply Unit NE2A-PD025 . . . . . (6)	The NE2A-PD025 Power Supply Unit is required when one or more Communications Units are mounted.
	DeviceNet Safety Unit NE2A-DNS21. . . . . (7)	The NE2A-DNS21 DeviceNet Safety Unit is mounted to the NE2A-series Controller. It supports both DeviceNet Safety and DeviceNet Standard Communications.
	EtherNet/IP Safety Unit NE2A-ENS21. . . . . (8)	The NE2A-ENS21 EtherNet/IP Safety Unit is mounted to the NE2A-series Controller. It supports both EtherNet/IP Safety and EtherNet/IP Standard Communications.
Network Configurator WS02-CFSC1-J . . . . . (9)		The Network Configurator is a software application for configuring Safety Control Systems. It can be used to set parameters for OMRON Safety Devices (including the NE2A) and for building CIP networks (including DeviceNet Safety and EtherNet/IP Safety).
NE1A Series	NE1A-SCPU01-V1 . . . . . (10) NE1A-SCPU02	The NE1A-SCPU01-V1 and NE1A-SCPU02 are the parts of Safety Controllers that control safety according to Safety Programs. They provide a DeviceNet interface and support DeviceNet Safety Communications.
NE0A Series	NE0A-SCPU01	The NE0A-SCPU01 is a small Safety Controller that supports logic operations and Safety Communications Slave functionality.
DST1 Series	Safety I/O Terminal (12 Safety Inputs) DST1-ID12SL-1 . . . . . (11)	The Safety I/O Terminals are Remote Safety I/O Slaves with safety functions. With a DeviceNet interface, they support DeviceNet Safety Slave functionality, and they exchange Safety I/O data with DeviceNet Safety Masters. The DST1-XD0808SL-1 supports logic operations, enabling local outputs to be directly controlled without the need for Safety Controller logic.
	Safety I/O Terminal (8 Safety Inputs, 8 Safety Outputs) DST1-MD16SL-1	
	Safety I/O Terminal (4 Safety Inputs, 4 Safety Relay Outputs) DST1-MRD08SL-1	
	Safety I/O Logic Terminal (8 Safety Inputs, 8 Safety Outputs) DST1-XD0808SL-1	
CS/CJ-series PLCs	CS1/CJ1 CPU Units . . . . . (12)	These OMRON PLCs are for Standard Control only. Mounting a CS/CJ-series DeviceNet Unit or CS/CJ-series EtherNet/IP Unit enables Standard I/O Communications or message communications with the NE2A-series Controller. The CJ2 CPU Units support programming with variables, so the same variable can be used as for the NE2A-series Controller.
	CJ2 CPU Units	

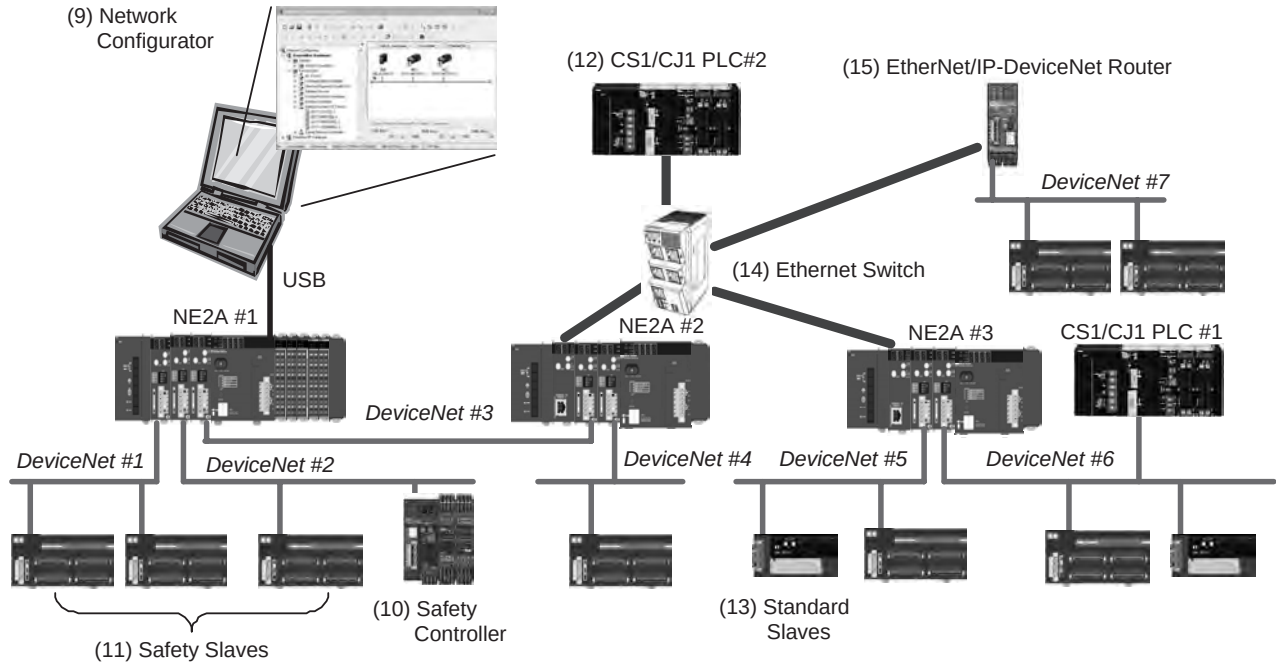
Series name, product name, model number		Description
OMRON DeviceNet Slave . . . . . (13)		The DeviceNet Slave is a Remote I/O Slave that supports DeviceNet Standard Communications, such as with the DRT2. It exchanges Standard I/O Data with a DeviceNet Master.
W4S1 Series	EtherNet/IP compatible Layer 2 Switching Hub . . . . . (14)	This is an OMRON EtherNet/IP compatible Ethernet switching hub with QoS functionality. The following three models are available. Each has a different number of LAN ports. 3 ports: W4S1-03B, 5 ports: W4S1-05B/C
NE1A-EDR01 EtherNet/IP-DeviceNet Router (“ED Router”) . . . . . (15)		This is a router designed for factory automation. It routes Safety Communications data and messages between EtherNet/IP and DeviceNet networks. The ED Router can be connected to an EtherNet/IP Safety Unit to enable Safety Communications and message communications between the EtherNet/IP Safety Unit and DeviceNet Safety Slaves (or NE1A-SCPU-series Safety Network Controllers that support safety slave functionality) that are connected to the ED Router.

Configuration for an NE2A-series Controller



- The maximum number of I/O Units is 20, including Safety Input Units and Safety Output Units.
- The maximum number of Communications Units is 6, including DeviceNet Units and EtherNet/IP Units. (Up to three EtherNet/IP Units can be connected.) A Power Supply Unit is required when one or more Communications Units are mounted.

System Configuration with an NE2A-series Controller



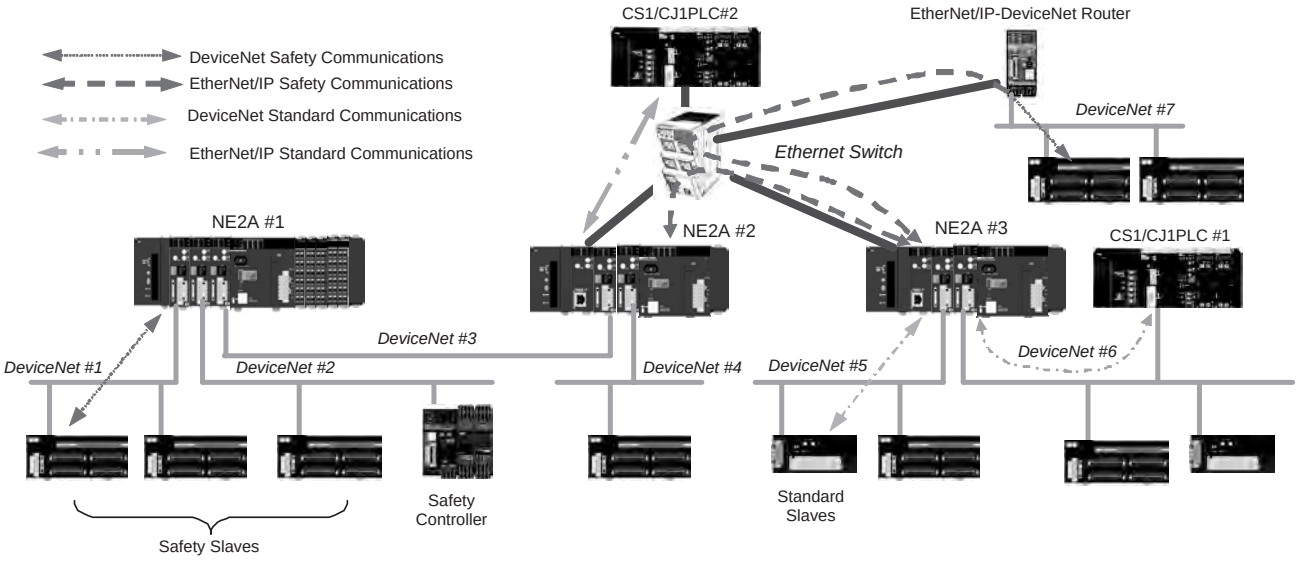
2-2 Safety Control System Configuration

This section describes the points to be considered and the restrictions when determining the system configuration.

2-2-1 Network System Configuration

The following communications networks can be used by the NE2A-series Controllers: DeviceNet Safety Communications, DeviceNet Standard Communications, EtherNet/IP Safety Communications, and EtherNet/IP Standard Communications.

Controller signals can be monitored from a Standard PLC. This makes it possible to build a system that integrates device control and Safety Control.



Selecting Networks

The following table shows the special features and the restrictions for each of the communications methods.

Select the optimum network based on considerations such as the communications distance between the Controllers and Standard PLCs, or between two Controllers, and the amount of data that is to be sent and received.

Item	EtherNet/IP	DeviceNet			
Connection configuration	Star configuration *1	The multi-drop and T-branch connections can be combined (for main lines and branch lines).			
Baud rate	100 or 10 Mbps	500, 250, or 125 kbps			
Communications distance	100 m With switching hubs, there is no limit on the number of cascade connections.	**Baud rate**	**Network length**	**Branch length**	**Total branch length**
		500 kbps	100 m max. (100 m max.)	6 m max.	39 m max.
		250 kbps	250 m max. (100 m max.)	6 m max.	78 m max.
		125 kbps	500 m max. (100 m max.)	6 m max.	156 m max.
		The numbers in parentheses are for Thin Cable.			
Nodes per network	256 max. (maximum number that can be set by the Network Configurator)	64 max.			

Item	EtherNet/IP	DeviceNet
Safety Masters	128 connections/Unit 32 bytes/connection	64 connections/Unit 16 bytes/connection
	Maximum total of 160 CIP Safety Master connections per NE2A-series CPU Unit	
Safety Slaves	8 connections/Unit 32 bytes/connection	4 connections/Unit 16 bytes/connection
	Maximum total of 32 CIP Safety Slave connections per NE2A-series CPU Unit	
Standard Masters	No Originator function	126 connections (63 Slaves)/Unit 2 connections/Slave 16 input and 16 output bytes/connection 4 protocols supported: poll, bit-strobe, COS, cyclic
Tag Data Links per Standard Slave	Target function supported. 2 connections/Unit 1,024 bytes/connection	2 connections/Unit 200 input and 200 output bytes/connection

*1 An Ethernet Switching Hub is required for an EtherNet/IP configuration. For details on Ethernet Switching Hubs, refer to *5-10 Selecting the Ethernet Switching Hub*.

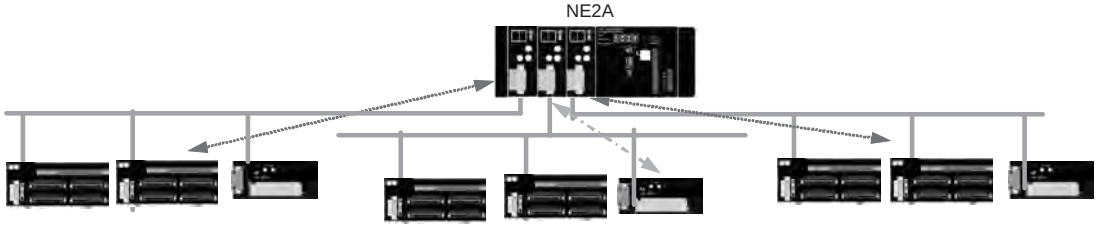
Selecting Centralized or Distributed Control

Select either centralized or distributed control for the system configuration.

Up to six Communications Units (DeviceNet Units or EtherNet/IP Units) can be mounted to one NE2A-series Controller. (Up to three EtherNet/IP Units can be connected.)

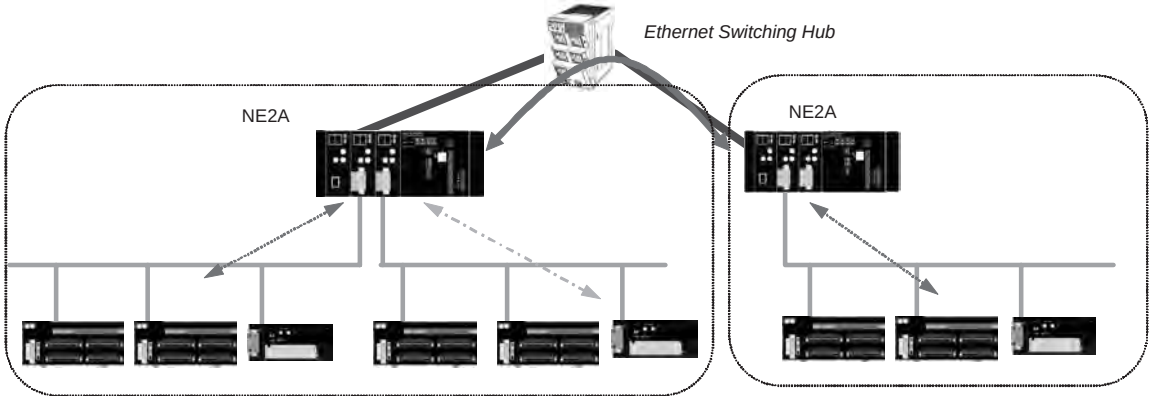
■ Centralized Control

Multiple networks can be used with an NE2A-series Controller, so distributing Slaves can reduce the bandwidth used per network and improve responsiveness in addition to expanding the Safety Control Area.



■ Distributed Control

Safety I/O Communications can be executed between NE2A-series Controllers by means of a high-speed EtherNet/IP Safety Network.



Comparison of the Above System Configurations

Configuration	Advantages	Disadvantages
Centralized control	• Low cost • Simple system management	• Limited distance compared to distributed control
Distributed control	• Long distance • Partial startup and adjustment are possible. • Improved responsiveness within each area	• High cost • Complex system management

Setting the Baud Rate

The baud rate is determined by the responsiveness required in the safety specifications and by the communications distance. The baud rate can be set to 500, 250, or 125 kbps for DeviceNet, or to 100 or 10 Mbps for Ethernet.

Set the same baud rate for all the nodes on the same network (Masters and Slaves). For details, refer to *3-6 DeviceNet Safety Units* and *3-7 EtherNet/IP Safety Units*.

Network Number and Node Address

An NE2A System can include multiple DeviceNet networks. Set network numbers and node addresses so that devices in the DeviceNet networks can be uniquely identified.

An NE2A System can also include multiple EtherNet/IP networks. Set IP addresses so that devices in the EtherNet/IP (Ethernet) networks can be uniquely identified.

For details, refer to *3-6 DeviceNet Safety Units*, *3-7 EtherNet/IP Safety Units*, and *5-2 Communications Specifications for NE2A-series Controllers*.

2-2-2 Connecting Safety Devices

Design the terminal parameters for the NE2A-series I/O Units and network Slaves to which the Safety Device are to be connected.

Depending on the required safety category, Safety Input device and Safety Output device wiring must be redundant and test outputs must be set.

Connecting to NE2A-series I/O Units

A maximum of 20 I/O Units can be connected to an NE2A-series Controller.

The maximum numbers of local I/O control points are as follows:

- Safety Inputs: 80
- Test Outputs: 40
- Safety Outputs: 80

Connectable Safety Input Devices

Refer to *6-2 Safety Input Functions*.

Connectable Safety Output Devices

Refer to *6-3 Safety Output Functions*.

Connecting to Network Slaves

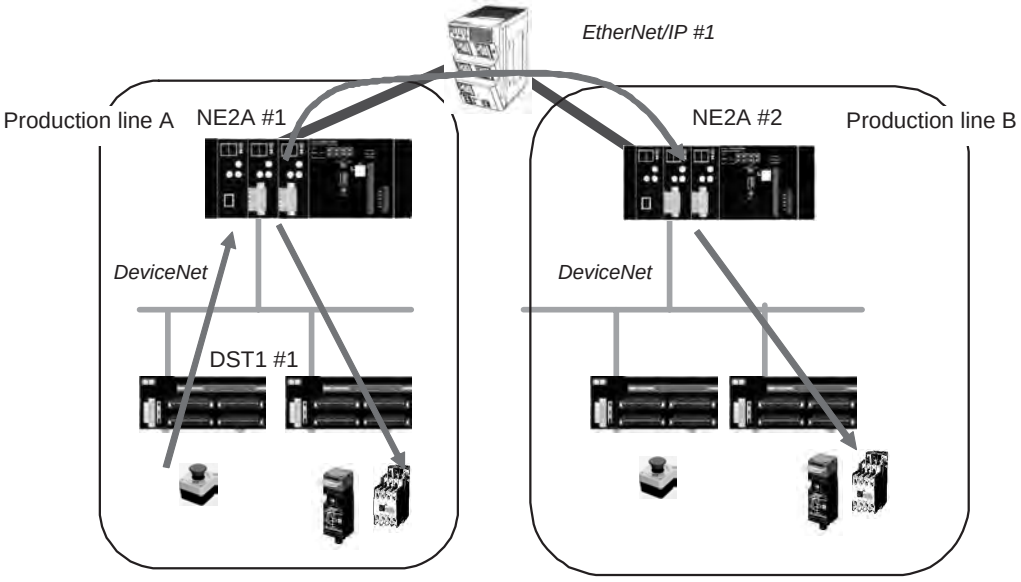
For details on the devices that can be connected to network Slaves, refer to the individual network Slave manuals.

2-2-3 Designing a Safety Control Interface

Design the signals for detecting the safety status, the stopping range for when safety cannot be confirmed, and the safety confirmation conditions and start signals at startup.

Design the Safety Data (assembly data) for sending Safety Signals between the NE2A-series Controller and network Slaves, and between NE2A-series Controllers. In addition, design the timing (connections) with the remote devices for sending and receiving the Safety Data.

For details, refer to *5-4 DeviceNet Safety Communications* and *5-6 EtherNet/IP Safety Communications*.



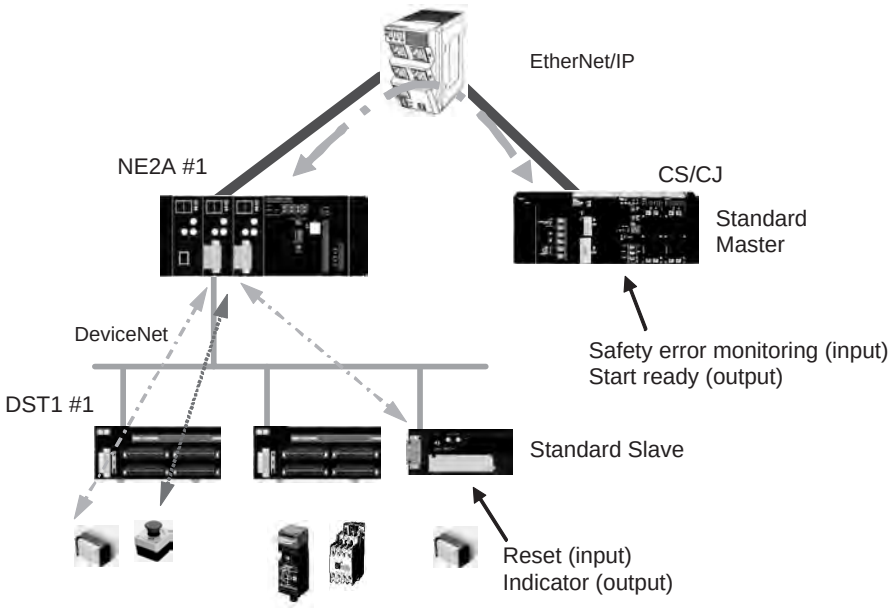
Production line A and production line B outputs are stopped by an emergency stop at production line A. The emergency stop is communicated from DST1 #1 to NE2A #1, and an emergency stop signal is set in the data from NE2A #1 to NE2A #2.

2-2-4 Designing a Standard Control Interface

By using the NE2A-series DeviceNet Safety Unit as the Master, Standard Control Data can be used for Safety Starting Signals between DeviceNet Slaves, for displays, etc. Also, NE2A-series Controller I/O and status can be monitored by a Standard PLC.

Design the Standard Data (assembly data) to be sent and received between the NE2A-series Controller and the network Slaves, and between the NE2A-series Controller and the Standard PLC. In addition, design the timing (connections) with the remote devices for sending and receiving the Standard Data.

For details, refer to *5-5 DeviceNet Standard Communications* and *5-7 EtherNet/IP Standard Communications*.


EtherNet/IP
NE2A #1
CS/CJ
Standard
Master
DeviceNet
Safety error monitoring (input)
Start ready (output)
DST1 #1
Standard Slave
Reset (input)
Indicator (output)

2-3 Designing Response Performance

2-3-1 Verifying the Network Bandwidth

Verify that the bandwidths used for DeviceNet and EtherNet/IP communications do not exceed the bandwidth allowed for the network.

The bandwidth is the network communications load. A communications timeout will occur in any communications for which connections are set that exceed the allowable usage ratio for communications.

If the allowable bandwidth for the network is exceeded, change the network configuration.

For details, refer to *8-2 Calculating Safety Response Performance*.

2-3-2 Verifying Safety Response Performance (Reaction Times)

The safe distance is calculated based on the reaction time. The reaction time is the maximum time required to stop an output in a safety chain[*1], taking into account the occurrence of interference and failure.

*1 Safety chains are logical connections for actualizing safety functions, from input devices to control devices (including remote I/O devices) to output devices.

Calculate all the reaction times and verify that they meet the specifications. If they do not meet the specifications, change the network configuration.

For details, refer to *8-2 Calculating Safety Response Performance*.

⚠ WARNING

Serious injury may possibly occur due to loss of required safety functions. Always confirm that the reaction time calculated for each safety chain satisfies the required specifications.



2-3-3 Verifying Response Performance in Standard Communications

Response Performance in DeviceNet Standard Communications

Response performance in DeviceNet Standard Communications is determined by the communications cycle time, the Slave communications time for each Slave, and the refresh processing time.

For details, refer to *8-3 Calculating Response Performance of Standard Communications*.

EtherNet/IP Tag Data Link Response Performance

With EtherNet/IP Tag Data Links, the data transmission period is set as a package interval (RPI) for each connection.

A delay occurs from when each node sends a packet until the packet reaches the destination node. The delay varies depending on factors such as the Tag Data Link connection settings (the number of connections and the data size), the number of nodes, the Switching Hubs to be used, and the cable length.

For details, refer to *8-3 Calculating Response Performance of Standard Communications*.

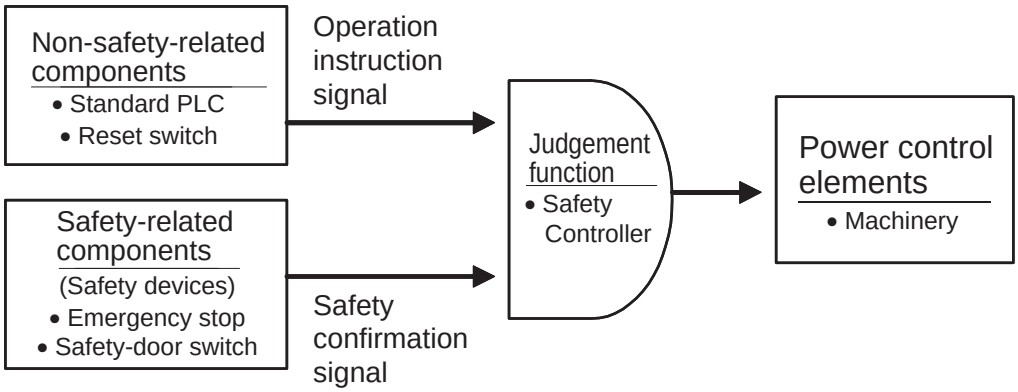
2-4 Designing Safety Control Logic

2-4-1 Designing the Program

Designing a Basic Program

Design interlock signals so that control devices can perform the following operations.

- Start the machinery only if safety can be confirmed when an operation instruction signal is input.
- Stop the machinery if safety cannot be confirmed.
- Design the system so that the stopped machinery can be restarted by a method such as a manual reset switch once the safety functions are operating.

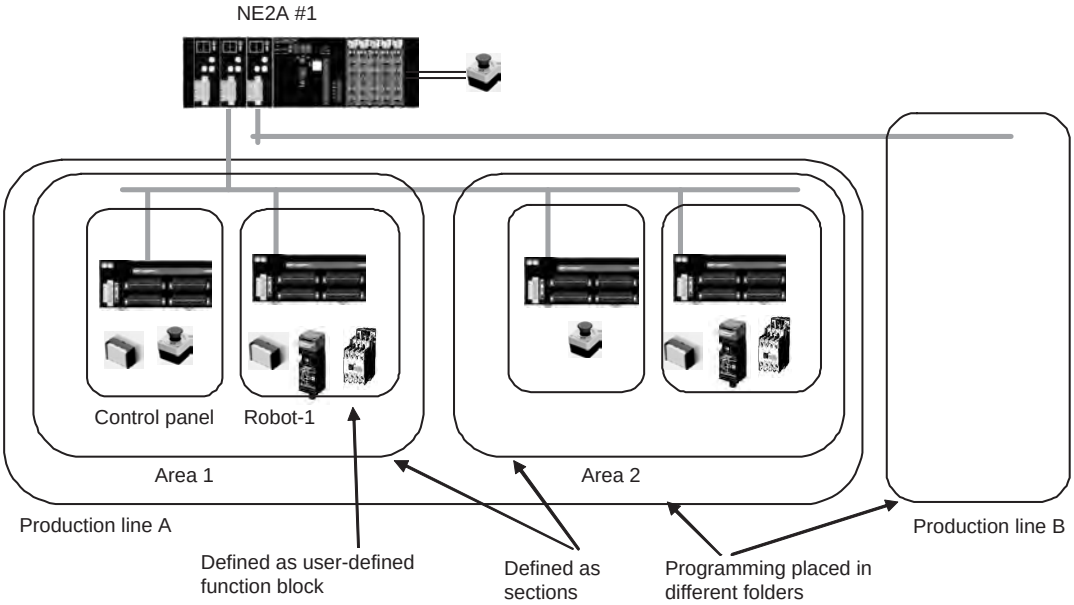


Structured Design

By structuring and modularizing the system, including the arrangement of local and remote I/O Safety Devices, the design can be streamlined and maintenance made easier.

With the Logic Editor for the NE2A-series Controller, sections and user-defined function blocks can be used as program components.

For details, refer to *4-4 Creating Programs*.



2-4-2 Programming with Variables

NE2A-series Controller program reusability is improved by using variables in programming.

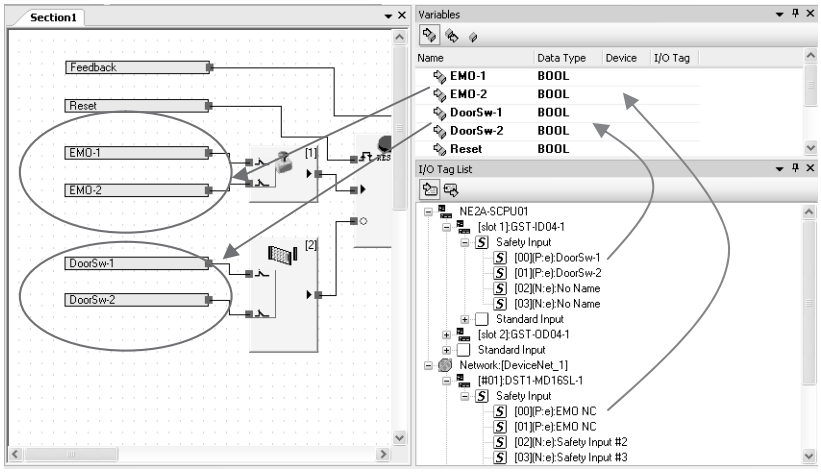
- Programming can be performed without having to consider whether a Safety Device is connected to an I/O Unit or to a Slave on the network.
- Once a program has been created, it does not have to be changed when the system configuration is changed.

For details, refer to *4-3 Creating Variables*.

Creating Variables

Either of the following two methods can be used to create variables.

- Creating variables while the I/O is still undefined.
  I/O tags can be linked to variables after a program has been created. This allows a program created with variables to be reused as a programming component.
- Creating variables from a list of defined I/O tags.
  This method saves time, because variable names are defined automatically and the variables are linked to the I/O tags.



Local I/O and remote I/O can be allocated to variables after completing the program.

Types of Variables

The following types of variables can be used. They can be linked to the I/O signals indicated in the table.

Type	Description
Input variables	Variables that can be linked to the following signals: • Local inputs: Signals of Safety Input device connected to NE2A-series Safety Input Units • Remote inputs: Signals of Safety Input device connected to Slaves on the network • Status: NE2A-series Controller internal status signals
Output variables	Variables that can be linked to the following signals: • Local outputs: Signals of Safety Output device connected to NE2A-series Safety Output Units • Remote outputs: Signals of Safety Output device connected to Slaves on the network

Type	Description
Internal variables	Variables that can be used only in programming. They cannot be linked to local I/O, remote I/O, or status.
System input variables	Variables with specific functions assigned in advance. The names of the system input variables cannot be changed and the system input variables cannot be deleted. • Always ON. • Always OFF. • ON for one cycle at operation startup.

For details on linking variables and I/O signals, refer to *4-3 Creating Variables*.

The same I/O tag can be assigned to more than one variable.

2-5 Managing Operation

2-5-1 Restricting Access to Safety Control Systems

Safety control system operation and maintenance must be performed under the supervision of a manager. Equipment safety can be protected by restricting access to Safety Control Systems.

This section describes the security functions for protecting Safety Control Systems from changes that the manager did not approve.

For details, refer to *7-1 Access Control with Passwords*.

Protecting Safety Control Systems after Operation Has Been Checked

After the operation of a Safety Control System has been checked, the configuration data can be locked to protect it from changes that the manager did not approve.

A locked Safety Control System cannot be stopped by an operator who does not know the password to unlock it, and configuration data cannot be changed.

Restricting Access to Safety Control Systems

With the NE2A-series Controllers, access to Safety Control Systems can be restricted by the person in charge by setting passwords for the following items.

- Project files
- Parameters (including programs)
- Devices

For details, refer to *7-3 Examples of Security According to Roles*.

2-5-2 Using Memory Cards to Download and Lock Parameters

With NE2A-series Controllers, a Memory Card can be used to set parameters and lock the configuration for devices in the NE2A System.

For details, refer to *7-2 Operation and Maintenance Using a Memory Card*.

SECTION 3
Configuration Unit Specifications and Nomenclature

This section provides the specifications and describes the nomenclature of the Units used in a NE2A-series Safety Network Controller.

3-1 General Specifications of NE2A-series Controllers 33
3-1-1 General Specifications of NE2A-series Controllers 33
3-1-2 Dimensions and Weights 34
3-2 Safety CPU Unit 35
3-2-1 Nomenclature 35
3-2-2 Indicators 35
3-2-3 Switches 37
3-2-4 Interfaces. 39
3-2-5 General Specifications 40
3-2-6 Dimensions (Reference Values) 40
3-3 End Cover 41
3-3-1 Nomenclature 41
3-3-2 Dimensions (Reference Values) 41
3-4 End Unit 42
3-4-1 Nomenclature 42
3-4-2 Dimensions (Reference Values) 42
3-5 Power Supply Unit 43
3-5-1 Nomenclature 43
3-5-2 Indicators 43
3-5-3 Interface 44
3-5-4 General Specifications 44
3-5-5 Dimensions (Reference Values) 45
3-6 DeviceNet Safety Units. 46
3-6-1 Nomenclature 46
3-6-2 Indications. 47
3-6-3 Switches 48
3-6-4 Interface 49
3-6-5 General Specifications 50
3-6-6 Dimensions (Reference Values) 50
3-7 EtherNet/IP Safety Units. 51
3-7-1 Nomenclature 51
3-7-2 Indications. 52
3-7-3 Switches 54
3-7-4 Interface 55
3-7-5 General Specifications 55
3-7-6 Dimensions (Reference Values) 56

3-8 Safety Input Units 57
3-8-1 Nomenclature and Terminal Layout 57
3-8-2 Indicators 58
3-8-3 I/O Specifications 58
3-8-4 I/O Terminals and Internal Connection Diagram 59
3-8-5 Wiring I/O Devices 59
3-8-6 Dimensions (Reference Values) 61
3-9 Safety Output Units 62
3-9-1 Nomenclature and Terminal Layout 62
3-9-2 Indicators 63
3-9-3 I/O Specifications 63
3-9-4 Output Terminals and Internal Connection Diagram 64
3-9-5 Power Supply Terminal Wiring and Wiring I/O Terminals. 64
3-9-6 Dimensions (Reference Values) 66

3-1 General Specifications of NE2A-series Controllers

3-1-1 General Specifications of NE2A-series Controllers

Item		Specifications
Power supply voltage	Unit power supply V0	20.4 to 26.4 VDC (24 VDC, –15% to +10%)
	Input circuit power supply V1	20.4 to 26.4 VDC (24 VDC, –15% to +10%)
	Output circuit power supply V2	20.4 to 26.4 VDC (24 VDC, –15% to +10%)
Current consumption	Unit power supply V0	1.2 A max. (with 20 I/O Units connected)
		CPU Unit: 300 mA
		I/O Units: 45 mA/Unit
	Input circuit power supply V1	60 mA/Unit max.
	Output circuit power supply V2	0.5 A/point max. and 1.2 A/Unit max.
Insulation class		Class lll (SELV)
Overvoltage category		II
Noise immunity		Compliant with IEC 61131-2
Vibration resistance		0.35 mm at 5 to 8.4 Hz, 9.8 m/s^2 at 8.5 to 150 Hz
Shock resistance		150 m/s^2 for 11 ms
Mounting		DIN Track (TH35-7.5/TH35-15 according to IEC 60715)
Ambient operating temperature		0 to 55°C
Ambient operating humidity		10% to 95% (with no condensation)
Ambient storage temperature		–40 to 70°C
Ambient operating environment		No corrosive gases
Degree of protection		IP20
Serial interface		USB version 1.1
Number of connectable I/O Units		20 max. (excluding End Units)
Number of connectable Communications Units		6 max. (A Power Supply Unit is required when a Communications Unit is connected.)

V0: This is the power supply for the internal control circuits of the Units. The power is supplied from the CPU Unit to the Safety Slice I/O Units and Communications Units.

V1: This is the power supply for the external input circuits and test output circuits of the Safety Input Units. Supply power to the V1 terminal of the CPU Unit. Power is supplied from the CPU Unit to the Safety Input Units. It is not necessary to supply power if Safety Input Units are not used.

V2: This is the power supply for the external output circuits of the Safety Output Units. The V2 and G2 terminals are independent on each Safety Output Unit, so supply power to the V2 and G2 terminals of each Safety Output Unit.

The following terminals are isolated form each other: V0 to G0, V1 to G1, and V2 to G2.

Note Power Supply Differentiation

V0 to G0: For internal logic circuits

V1 to G1: For external input devices and test outputs

V2 to G2: For external output devices. Power must be input to V2 and G2 on each Unit.

3-1-2 Dimensions and Weights

Without an External Power Supply Unit (No Communications Unit Connected)

Connection Configuration

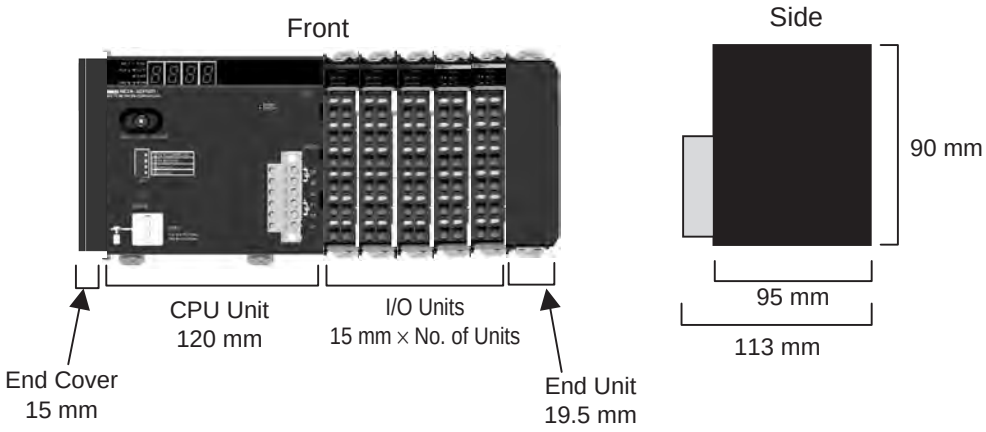
- Safety Input Units: A Units, Safety Output Units: B Units (A + B ≤ 20)

■ **Overall width (mm) = 154.5 + 15 × (A + B)**

■ **Height: 90 mm**

■ **Depth: 113 mm (including connectors)**

■ **Weight (g) = 500 × 90 × A + 95 × B**



With an External Power Supply Unit (Communications Unit Connected)

Connection Configuration

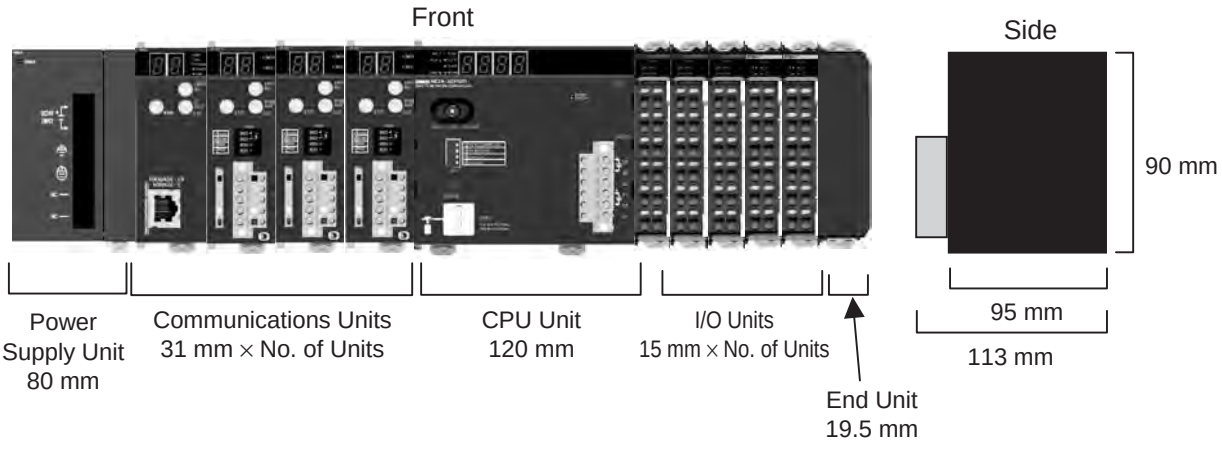
- Safety Input Units: A Units, Safety Output Units: B Units (A + B ≤ 20)
- DeviceNet Units: C Units, EtherNet/IP Units: D Units
  (C ≤ 6, D ≤ 3, C + D ≤ 6)

■ **Overall width (mm) = 219.5 + 15 × (A + B) + 31 × (C + D)**

■ **Height: 90 mm**

■ **Depth: 113 mm (including connectors)**

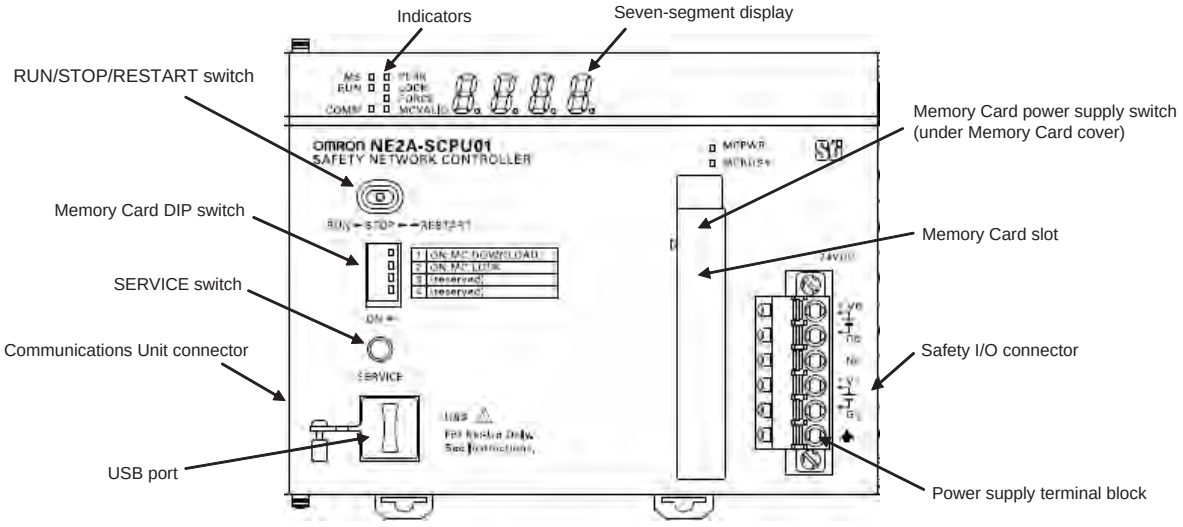
■ **Weight (g) = 850 + 90 × A + 95 × B + 118 × C + 100 × D**



3-2 Safety CPU Unit

3-2-1 Nomenclature

NE2A-SCPU01



3-2-2 Indicators

Indicators

The status indicators on the NE2A-series Safety CPU Unit show the operating status of the Safety CPU Unit, program, and Memory Card.

Indicator name	Color	Meaning
MS (Module Status)	Green /red	Indicates the operating status of the CPU Unit.
RUN	Green	Lit when the program is being executed.
FORCE	Yellow	Lit when force-setting/resetting enabled.
PERR	Red	Lit when there is a program error.
LOCK	Yellow	Lit when the configuration is locked.
COMM	Yellow	Flashing when USB data is being sent or received.
MC VALID	Yellow	Lit when the user has verified that the intended Memory Card is inserted.
MC PWR	Green	Lit when power is being supplied to the Memory Card. Do not remove the Memory Card while power is being supplied.
MC BUSY	Yellow	Lit when data is being read from or written to the Memory Card. Do not remove the Memory Card or turn OFF the Unit power supply while this indicator is lit.

Indicator Status and Meaning

Indicator name	Color	Status	Meaning
MS	Green	ON	RUN mode
		Flashing	IDLE mode
	Red	ON	Critical fault status (a fatal error has occurred) or a Communications Unit is connected without a Power Supply Unit. (See note.)
		Flashing	Abort status (A non-fatal error has occurred.) (See note.)
	Green/red	Flashing	Waiting for configuration. Alternatively, CONFIGURATION RESTORE Mode.
	-	OFF	V0-G0: Power is not being supplied to the internal control circuits.
RUN	Green	ON	Program running.
		OFF	Program stopped.
FORCE	Yellow	ON	Force-setting/resetting enabled.
		OFF	Force-setting/resetting disabled.
PERR	Red	ON	The program has detected an error. Check the location of the error using the program monitor.
		OFF	The program has not detected an error or program execution is stopped.
LOCK	Yellow	ON	The configuration is valid and locked.
		Flashing	The configuration is valid but not locked. When the system is operating, lock the configuration using the Network Configurator or a Memory Card.
		OFF	There is no valid configuration. Download the configuration using the Network Configurator or a Memory Card.
COMM (USB)	Yellow	Flashing	Data transmission/reception in progress.
		OFF	No data transmission/reception in progress.
MC VALID	Yellow	ON	A validated Memory Card is inserted.
		OFF	A Memory Card is not inserted or the Memory Card has not been validated.
MC PWR	Green	ON	Power is being supplied to Memory Card. Turn OFF the power supply to the Memory Card before removing it.
		OFF	Power to the Memory Card is OFF.
MC BUSY	Yellow	ON	Memory Card access in progress.
		OFF	Memory Card access not in progress.

ON : ON Flashing : Flashing OFF : OFF

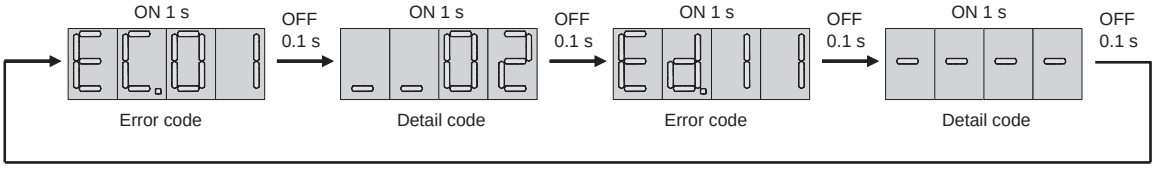
Note Refer to *SECTION 19 Troubleshooting* for information on handling errors.

Seven-segment Display

The 4-digit 7-segment display on the Safety CPU Unit shows the status and error codes for the NE2A-series Controller.

Status		Display
Normal operation	Operating mode: CONFIGURING	"----" displayed.
	Operating mode: RUN mode, IDLE mode	A 4-digit user-set ID number for the program in the NE2A-series Controller is displayed. The characters "----" will be displayed if a user program ID number has not been set.
	Operating mode: CONFIGURATION RESTORE Mode	The status of restoring the configuration is displayed. For details, refer to *SECTION 20 Inspections and Maintenance*.
Errors	CRITICAL FAULT Mode	The display will alternate between a 4-digit error code and a 4-digit detail code. For details, refer to *SECTION 19 Troubleshooting*. *1
	ABORT Mode	
	Non-fatal error	

*1 Seven-segment Display When an Error Occurs



⚠ WARNING

Serious injury may possibly occur due to loss of required safety functions. Do not use the NE2A-series Controller's indicators for Safety Operations.

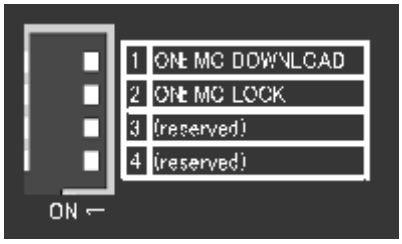
3-2-3 Switches

Memory Card DIP Switch

Set the function of the Memory Card by using the DIP switch on the front of the NE2A-series Safety CPU Unit.

The processing that is set on the Memory Card DIP switch will be executed when you press the SERVICE switch, which is described in the following section.

Set all the pins to OFF if the Memory Card functions will not be used.



Pin	Name	Default	Description
1	MC DOWNLOAD	OFF	The system will start in CONFIGURATION RESTORE Mode when the power supply is turned ON. In this mode, the configuration can be restored using the Memory Card. *1
2	MC LOCK	OFF	The system will start in CONFIGURATION RESTORE Mode when the power supply is turned ON. In this mode, the configuration can be restored using the Memory Card. *1
3	(Reserved)	OFF	Leave set to OFF (for future expansion).
4	(Reserved)	OFF	Leave set to OFF (for future expansion).

*1 For details, refer to *7-2 Operation and Maintenance Using a Memory Card*.
If MC DOWNLOAD (pin 1) and MC LOCK (pin 2) are both ON, a fatal error (abort) will occur in the CPU Unit.

Note Be sure to turn OFF the power supply to the NE2A-series Controller before setting the Memory Card DIP switch.

SERVICE Switch

The SERVICE switch is used in CONFIGURATION RESTORE Mode.

Do not press this switch if the configuration function is not being used.

For details, refer to *7-2 Operation and Maintenance Using a Memory Card*.



RUN/STOP/RESTART Switch

This switch is used to execute or stop a program or to restart the NE2A-series Controller.

To enable using this switch, a Memory Card with an operation rights file on it must be inserted into the CPU Unit.

For details, refer to *7-2 Operation and Maintenance Using a Memory Card*.



Changing between RUN and STOP

Program execution can be started or stopped by pressing the RUN/STOP/RESTART switch.

Also, the system settings can be used to start or stop program execution for all the NE2A/NE1A-series Controllers on the network at the same time.

The operating mode of the device can be changed by changing the switch only if the operating mode of the NE2A-series Controller and the switch position agree.

Example

If the switch is in the STOP position and the operating mode of the NE2A-series Controller is RUN, the operating mode of the device will not change even if the switch is changed from STOP to RUN. If the switch is in the STOP position and the operating mode of the NE2A-series Controller is STOP, the operating mode of the device will change if the switch is changed from STOP to RUN.

RESTART

The NE2A-series Controller will be restarted if the switch is pressed from the STOP position to the RESTART side for 1 s or longer. The switch will return to the STOP position.

Memory Card Slot

A special Memory Card can be inserted.

When you take out the Memory Card, use the following procedure to make sure that the power supply to the Memory Card is stopped.

1,2,3... 1. Press the Memory Card power supply switch.
2. Check that the MC PWR indicator turns OFF.

A Dust Cover is included.

Memory Card Models

Model	Memory capacity	Remarks
HMC-EF183	128 MBytes	The supported Memory Card format is FAT16.
HMC-EF283	256 MBytes	
HMC-EF583	512 MBytes	

Memory Card Power Supply Switch

This switch is used to stop the power supply to the Memory Card.

3-2-4 Interfaces

USB Port

The port complies with USB version 1.1.

USB bus power is not supplied.

A Dust Cover is included.

Power Supply Terminal Block

This terminal block is used to supply power for the internal circuits and input circuits.

■ Power Supply Terminal Block Signal Arrangement

Terminal	Function
V0	Power supply terminal for internal circuits (24 VDC)
G0	Power supply terminal for internal circuits (0 VDC)
NC	Not used (Do not connect.)
V1	Power supply terminal for input circuits (24 VDC)
G1	Power supply terminal for input circuits (0 VDC)
⏚	FG: Ground this terminal.

Note Do not use a cable that is longer than 3 m for the power supply.

Safety I/O Connector

This connector is connected to the first I/O Unit.

An End Cover must be attached if an I/O Unit is not connected.

Communications Unit Connector

This connector is connected to the first Communications Unit.

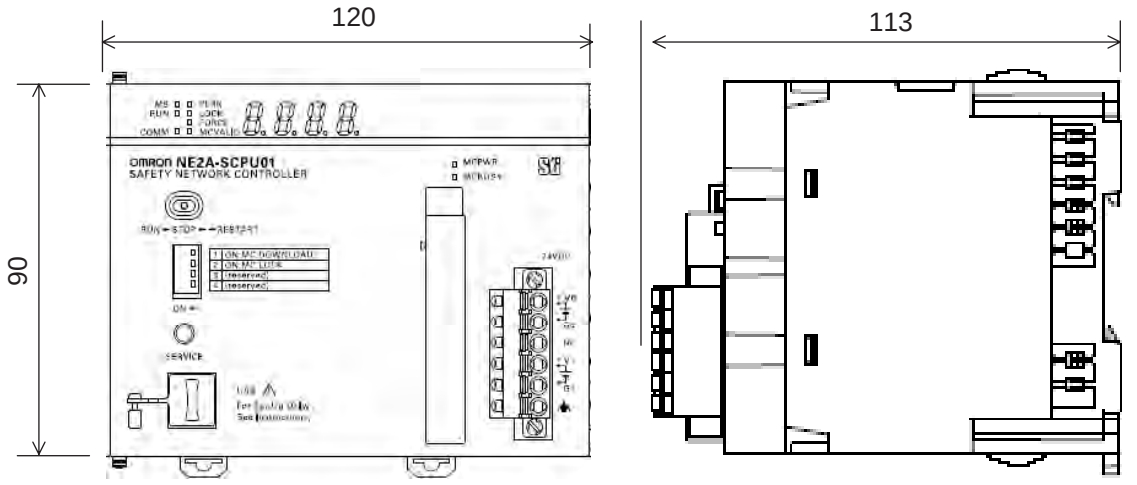
An End Cover must be mounted if a Communications Unit is not connected.

3-2-5 General Specifications

Refer to *3-1-1 General Specifications of NE2A-series Controllers*.

3-2-6 Dimensions (Reference Values)

Item	Specifications
Dimensions	120 × 90 × 113 mm (W × H × D)
Weight	415 g max.

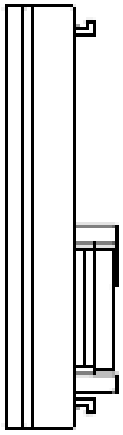


Unit: mm

3-3 End Cover

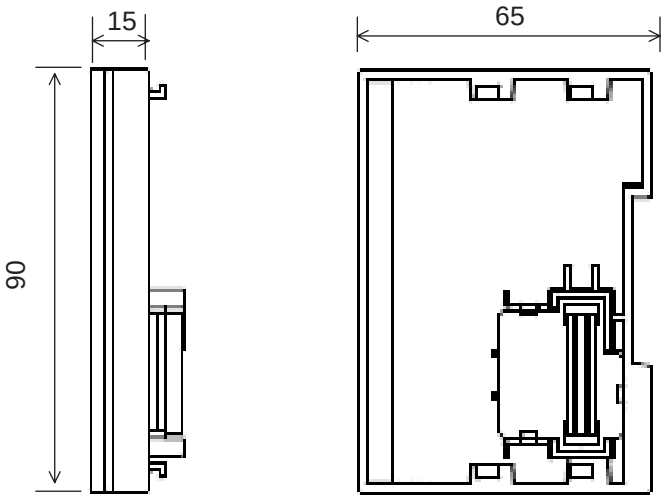
3-3-1 Nomenclature

NE2A-TER01



3-3-2 Dimensions (Reference Values)

Item	Specifications
Dimensions	15 × 90 × 65 mm (W × H × D)
Weight	30 g max.

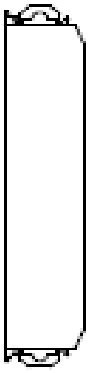


Unit: mm

3-4 End Unit

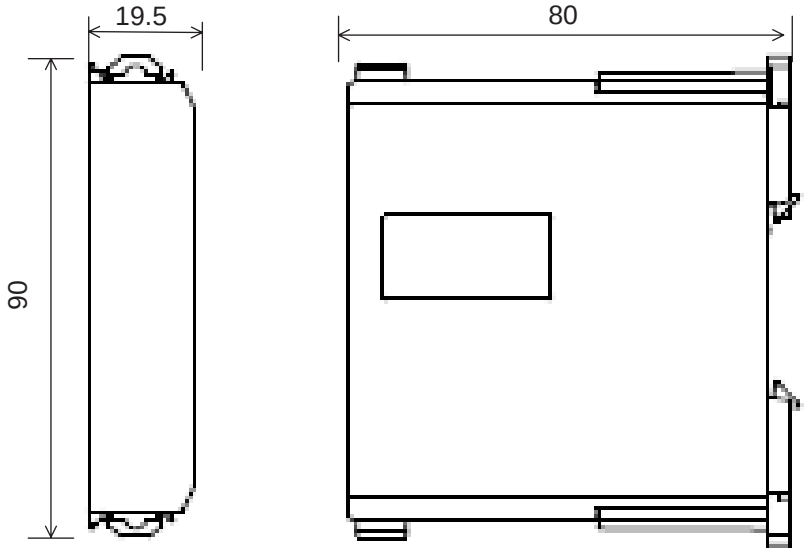
3-4-1 Nomenclature

NE2A-END



3-4-2 Dimensions (Reference Values)

Item	Specifications
Dimensions	19.5 × 90 × 95 mm (W × H × D)
Weight	55 g max.

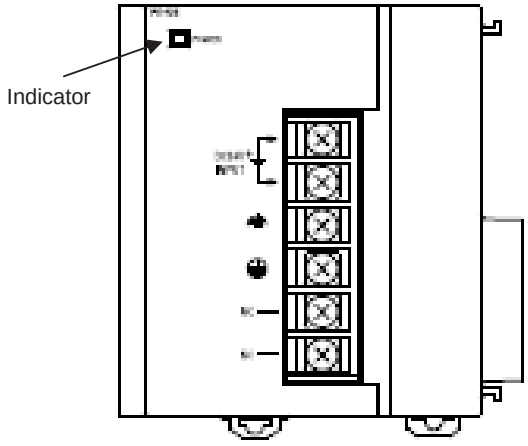


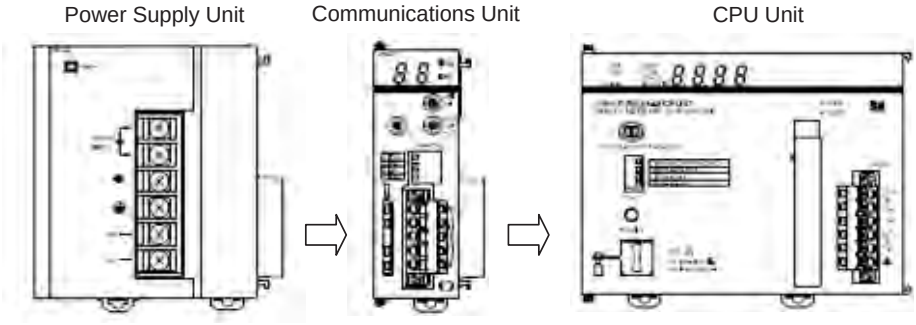
Unit: mm

3-5 Power Supply Unit

3-5-1 Nomenclature

NE2A-PD025





Power Supply Unit Connection Diagram

3-5-2 Indicators

Power

This indicator is lit when 5 VDC is output from the Power Supply Unit.

3-5-3 Interface

Terminal Block

■ **Power Supply Terminal Block Signal Arrangement**

Terminal	Function
DC 24V INPUT	Supplies 24-VDC power.
	LG: Ground separately to 100 Ω or less to provide stronger noise immunity and prevent electrical shock.
	GR: Ground separately to 100 Ω or less to help prevent electrical shock.
NC	Not used. (Do not connect.)

Note Do not use a cable that is longer than 3 m for the power supply.

Note The power supply input terminal block uses M4 self-rising screws. Tighten the terminal block screws to a torque of 1.2 N·m.

3-5-4 General Specifications

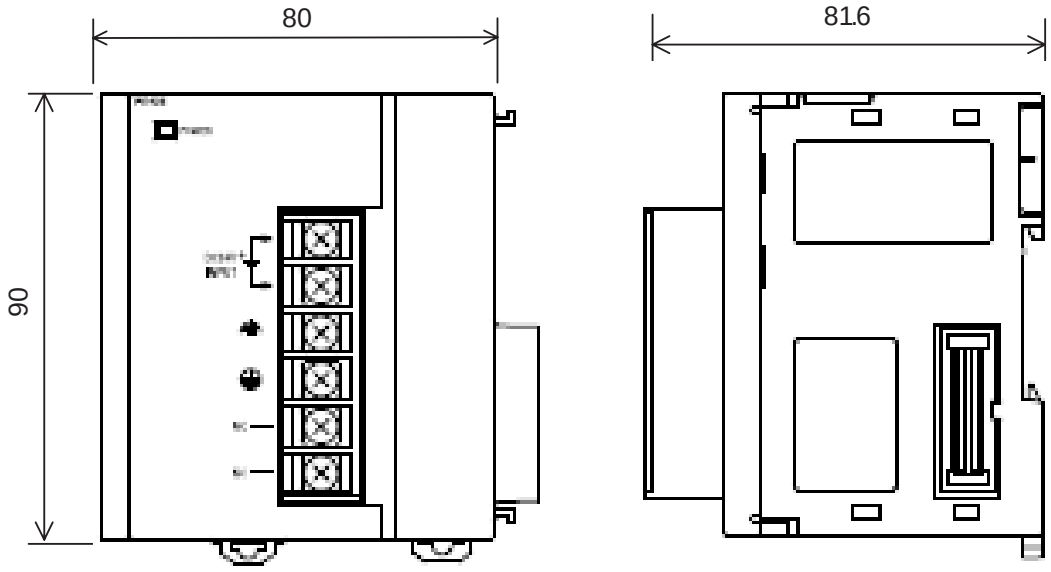
Item	Specifications
Power supply voltage	24 VDC
Allowable power supply voltage range/ operating frequency range	19.2 to 28.8 VDC
Current consumption	50 W max.
Inrush current	24-VDC input: 30 A max. (cold start) 20 ms max.
Power supply output capacity	5 VDC, 5.0 A
	24 VDC, 0.8 A
	25 W total
Insulation resistance	20 MΩ min. at 500 VDC (between all external DC terminals and GR terminal)
Dielectric strength	1,000 VAC, 50/60 Hz for 1 min with leakage current of 10 mA max. (between all external DC terminals and GR terminal)

Specifications that are not listed above conform to *3-1-1 General Specifications of NE2A-series Controllers*.

Note A Power Supply Unit must be mounted if one or more Communications Units are connected.

3-5-5 Dimensions (Reference Values)

Item	Specifications
Dimensions	80 × 90 × 81.6 mm (W × H × D)
Weight	380 g max.



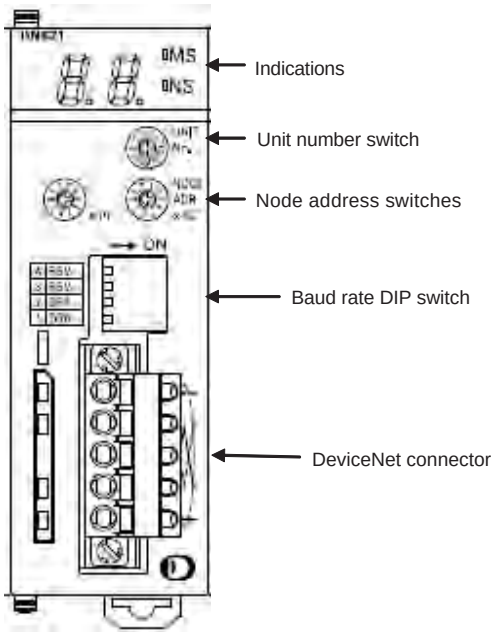
Unit: mm

3-6 DeviceNet Safety Units

The NE2A-DNS21 DeviceNet Safety Unit is for NE2A-series Controllers only. It cannot be mounted to a CJ-series PLC.

3-6-1 Nomenclature

NE2A-DNS21



3-6-2 Indications

MS/NS Indicators

Label	Indicator name	Color	Status	Operating status
MS	Module Status	---	■	• Power is not being supplied.
		Green	☐	• Normal operation.
		Red	◪ ON: 0.5 s OFF: 0.5 s	• Non-fatal error. *1 • Unit number setting error or error due to switches being changed during operation. *1
			☐	• Fatal error. If the error occurs again, the Unit must be replaced.
		Green/Red	◪ Lit green: 0.5 s Lit red: 0.5 s	• Waiting for configuration
NS	Network Status	---	■	• The Unit power is not being supplied. • Network power is not being supplied. • Offline.
		Green	◪ ON: 0.5 s OFF: 0.5 s	• Online connection to DeviceNet has not been established.
			☐	• The DeviceNet Safety Communications, DeviceNet Standard Communications, or message communications is online and at least one connection is established.
		Red	◪ ON: 0.5 s OFF: 0.5 s	• Safety I/O Communications error • Standard I/O Communications error
			☐	• Unable to communicate (Bus Off error or duplicated MAC ID error).

☐ : ON ◪ : Flashing ■ : OFF

*1 This error occurs when the switch is changed. The system will recover from the error when the switch is returned to the original setting. It is not necessary to turn OFF the power supply and reset the CPU Unit.

Seven-segment Display

Status	Display	Description
Normal operation	Node address	Node address (decimal) of local node
Error operation	Switches between error code and node address of error node	Switches between the error code (hexadecimal) and node address (decimal) of error node. The codes for all current errors are repeatedly displayed in order.

The characters "--" will flash while the configuration data is being saved to show that the data is being saved.

		Safety Master	Safety Slave	Standard Master	Standard Slave
No connections set		Lit	Lit	Lit	Lit
Connections set	Connection not established	Flashing	Lit	Flashing	Lit
	Connection established	Lit	Lit	Lit	Lit

The display will flash if both a “flashing” condition (e.g., Safety Master connection not established) and a “lit” condition (e.g., Standard Slave connection not established) occur at the same time.

3-6-3 Switches

Unit Number Rotary Switch

Use this switch to set the unit number of the DeviceNet Safety Unit.

Set the unit number so that the same unit number is not used for another Communications Unit mounted to the same CPU Unit.

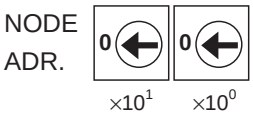


Value	Description
0 to F	Operation will be performed with the set unit number. The default setting is 0.

Note Set the switch using a small flat-head screw driver and be careful not to damage the rotary switch.

Node Address Switches

Use these switches to set the DeviceNet node address as a decimal number. Any node address can be set as long as it is not the same address as another node on the same network. A node address duplication error will occur and communications will stop an address that is already used by another node is set.



Set value	Description
00 to 63	Operation will be performed with the value set using the switches. The default setting is 63.
64 to 69	Do not set. (The Unit will not start.)

Be sure the power supply is turned OFF before setting these switches. The MS indicator will flash red and communications will be as follows:

- Safety I/O Communications will stop.
- Standard I/O Communications will continue.

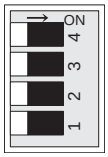
Safety I/O Communications will start again when the node address is returned to the original setting.

Note Set the switches using a small flat-head screw driver and be careful not to damage the rotary switches.

Baud Rate DIP Switch

Use this DIP switch to set the DeviceNet baud rate.

Set the same baud rate for all nodes (i.e., Masters and Slaves) on the same network.



Pin	Function
1	Baud rate (Refer to the following table.)
2	
3	Reserved
4	Reserved

Pin settings		Baud rate
1	2	
OFF	OFF	125 Kbit/s (default setting)
ON	OFF	250 Kbit/s
OFF	ON	500 Kbit/s
ON	ON	Do not set. (The Unit will not start.)

Be sure that the power supply is turned OFF before setting this DIP switch. If the baud rate is changed during operation, the MS indicator will flash red and communications will be as follows:

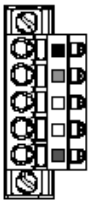
- Safety I/O Communications will stop.
- Standard I/O Communications will continue.

Safety I/O Communications will start again when the baud rate is returned to the original setting.

3-6-4 Interface

DeviceNet Connector

The DeviceNet connector is labeled with the colors of the wires in the DeviceNet cable. Check that wiring is correct by matching the colors of the wires in the DeviceNet cable with the colors of the labels. The following table gives the wire colors.



Color	Signal
Black	Negative power (V-)
Blue	Communications data low side (CAN L)
-	Shield
White	Communications data high side (CAN H)
Red	Positive power (V+)

Note

- Before connecting the DeviceNet cable, be sure to turn OFF the power supply to the NE2A-series Controller, the power supply to all nodes on the network, and the communications power supply.
- Secure the DeviceNet connector to the specified torque (0.25 to 0.3 N·m).
- Separate the DeviceNet cable from high-voltage lines and power lines.
- Used DeviceNet-compliant Thick Cables or Thin Cables for the communications cables. Do not use flat cables.

3-6-5 General Specifications

Item	Specifications
Operating voltage	Supplied from Power Supply Unit.
Current consumption	290 mA max.
DeviceNet communications power supply	24 VDC, 18 mA max. (supplied from DeviceNet connector)

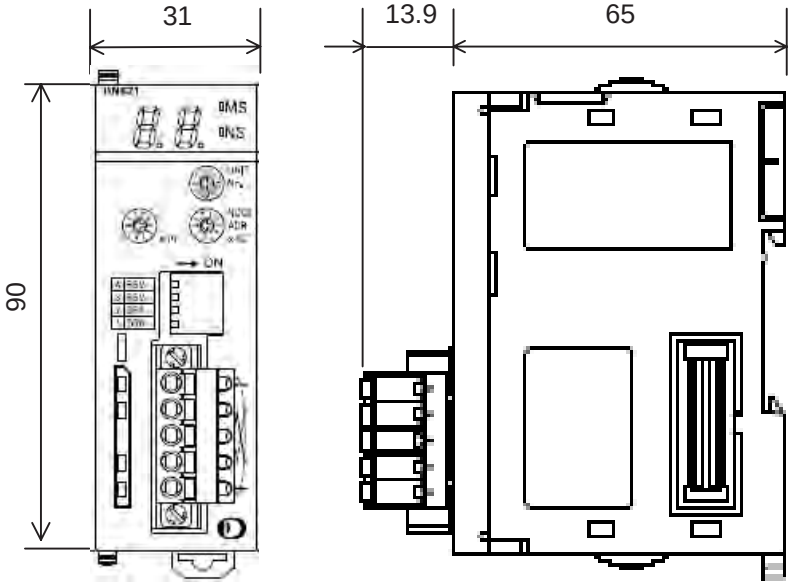
Specifications that are not listed above conform to *3-1-1 General Specifications of NE2A-series Controllers*.

Up to six DeviceNet Units can be connected to one NE2A-series Controller. Do not exceed the maximum of six Communications Units if DeviceNet Units and EtherNet/IP Units are both connected.

Note The maximum current consumption of the DeviceNet Safety Unit (NE2A-DNS21) is 290 mA. Connect a Power Supply Unit (NE2A-PD025) if one or more Communications Units are mounted to the NE2A-series CPU Unit.

3-6-6 Dimensions (Reference Values)

Item	Specifications
Dimensions	31 × 90 × 65 mm (W × H × D) (not including the DeviceNet connector)
Weight	118 g (including the enclosed connector)



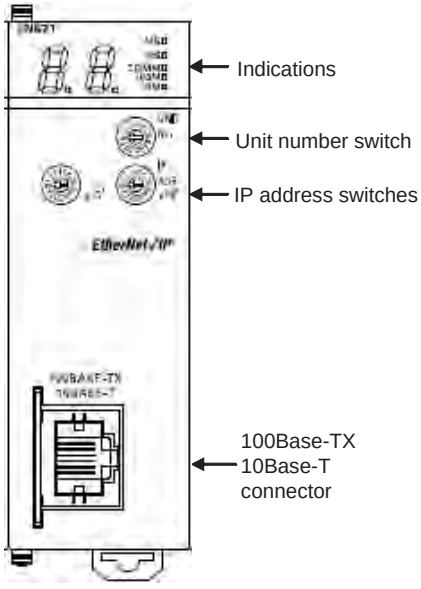
Unit: mm

3-7 EtherNet/IP Safety Units

The NE2A-series EtherNet/IP Unit (NE2A-ENS21) is for NE2A-series Controllers only. It cannot be mounted to CJ-series PLCs.

3-7-1 Nomenclature

NE2A-ENS21



3-7-2 Indications

MS, NS, COMM, 100M, and 10M Indicators

Label	Indicator name	Color	Status	Operating status
MS	Module Status	---	■	• Power is not being supplied.
		Green	☐	• Normal operation.
		Red	◪ ON: 0.5 s OFF: 0.5 s	• Non-fatal error *1 • Unit number setting error or error due to switches being changed during operation. *1
			☐	• Fatal error. If the error occurs again, the Unit must be replaced.
		Green/Red	◪ Lit green: 0.5 s Lit red: 0.5 s	• Waiting for configuration
NS	Network Status	---	■	• The Unit power is not being supplied. • Waiting for NE2A initialization to start. • Offline. *2
		Green	◪ ON: 0.5 s OFF: 0.5 s	• Not configured.
			☐	• The EtherNet/IP Safety Communications, EtherNet/IP Standard Communications, or message communications is online and at least one connection is established.
		Red	◪ ON: 0.5 s OFF: 0.5 s	• Safety I/O Communications error • Standard I/O Communications error
			☐	• Unable to communicate (duplicated IP addresses)
100M	100Mbps	Yellow	■	• 100Base-TX link not established.
			☐	• 100Base-TX link established.
10M	10Mbps	Yellow	■	• 10Base-T link not established.
			☐	• 10Base-T link established.
COMM	Communication	Yellow	■	• No data being sent or received.
			☐	• Data being sent or received.

☐ : ON ◪ : Flashing ■ : OFF

*1 This error occurs when the switch is changed. The system will recover from the error when the switch is returned to the original setting. It is not necessary to turn OFF the power supply and reset the CPU Unit.

*2 After startup, this indicator will not turn OFF if the node goes offline once it has gone online.

Seven-segment Display

Status	Display	Display description
Normal operation	Lower 8 bits of IP address	Lower 8 bits (hexadecimal) of IP address of local node
Error operation	Switches between error code and lower 8 bits of IP address for error node	Switches between the error code (hexadecimal) and lower 8 bits (hexadecimal) of the IP address for the error node. The codes for all the current errors are repeatedly displayed in order.

		Safety Master	Safety Slave	Standard Master	Standard Slave
No connection settings		Lit	Lit	---	Lit
Connection set	Connection not established	Flashing	Lit	---	Lit
	Connection established	Lit	Lit	---	Lit

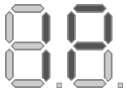
The display will flash if both a “flashing” condition (e.g., Safety Master connection not established) and a “lit” condition (e.g., Standard Slave connection not established) occur at the same time.

The characters “--” will flash while the configuration data is being saved to show that the data is being saved. Also, all digits of the IP address will be displayed at startup.

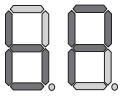
IP Address Display Example

After the display type, the IP address will be displayed flowing from right to left.

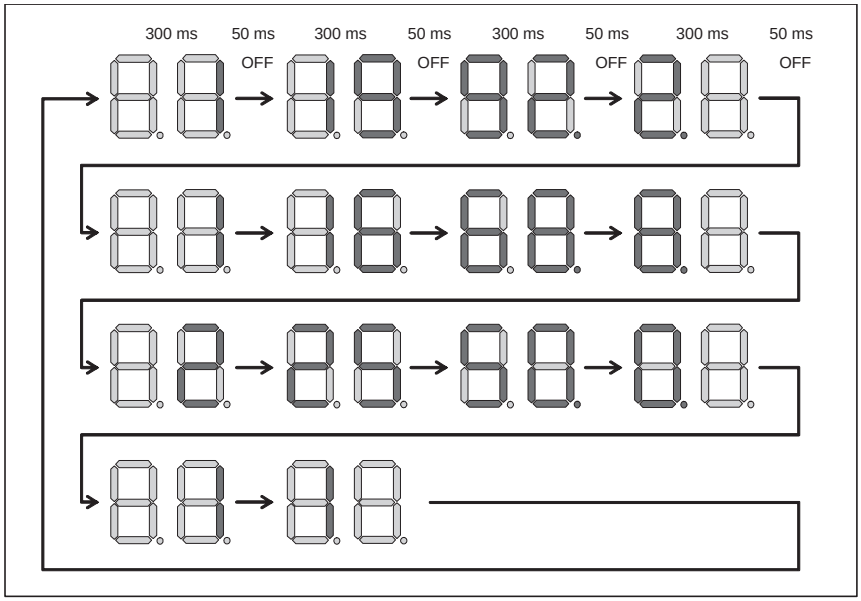
Display Type (IP Address for EtherNet/IP)



Display Type (IP Address for EtherNet/IP with BOOTP Setting)



Display Example for IP Address 192.168.250.1.



3-7-3 Switches

Unit Number Rotary Switch

Use this switch to set the unit number of the EtherNet/IP Unit. Set the unit numbers so that the same unit number is not used for another Communications Unit mounted to the same CPU Unit.



Value	Description
0 to F	Operation will be performed with the set unit number. The default setting is 0.

Note Set the switch using a small flat-head screwdriver and be careful not to damage the rotary switch.

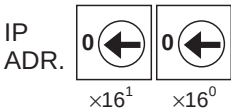
IP Address Switches

Use these switches to set the node address of EtherNet/IP as a hexadecimal number.

Each EtherNet/IP Units is identified by its IP address when there is more than one EtherNet/IP Unit connected to an Ethernet network.

Set a hexadecimal number on the IP address switches so that the same IP address is not used for other Ethernet devices that are connected to the same Ethernet network.

The IP address can be set from 01 to FE (1 to 254 decimal) as long as it is not used by another Ethernet device on the same network.



Value	Description
00	The IP address set using the Network Configurator will be used. If a BOOTP startup is set from the Network Configurator, BOOTP is used. The default setting is 00.
FF	BOOTP is used at startup.
01 to FE	The value of these switches is used as the host ID of the IP address. The value set with the Network Configurator is used for the network ID.

Be sure the power supply is turned OFF before setting these switches. If the IP address is changed during operation, the MS indicator will flash red and communications will be as follows:

- Safety I/O Communications will stop.
- Standard I/O Communications will continue.

Safety I/O Communications will start again when the IP address is returned to the original setting.

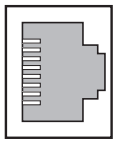
Note Set these switches using a small flat-head screwdriver and be careful not to damage the rotary switches.

3-7-4 Interface

Ethernet Connector

Use this connector to connect the Ethernet twisted-pair cable.

- Electrical specifications: Conform to IEEE 802.3 standards.
- Connector structure: RJ45 8-pin Modular Connector (conforms to ISO 8877)



Pin	Signal name	Abbr.	Signal direction
1	Transmission data+	TD+	Output
2	Transmission data–	TD–	Output
3	Reception data+	RD+	Input
4	Not used	-	-
5	Not used	-	-
6	Reception data–	RD–	Input
7	Not used	-	-
8	Not used	-	-
Connector hood	Frame ground	FG	-

3-7-5 General Specifications

Item	Specifications
Operating voltage	Supplied from the Power Supply Unit.
Current consumption	410 mA max.

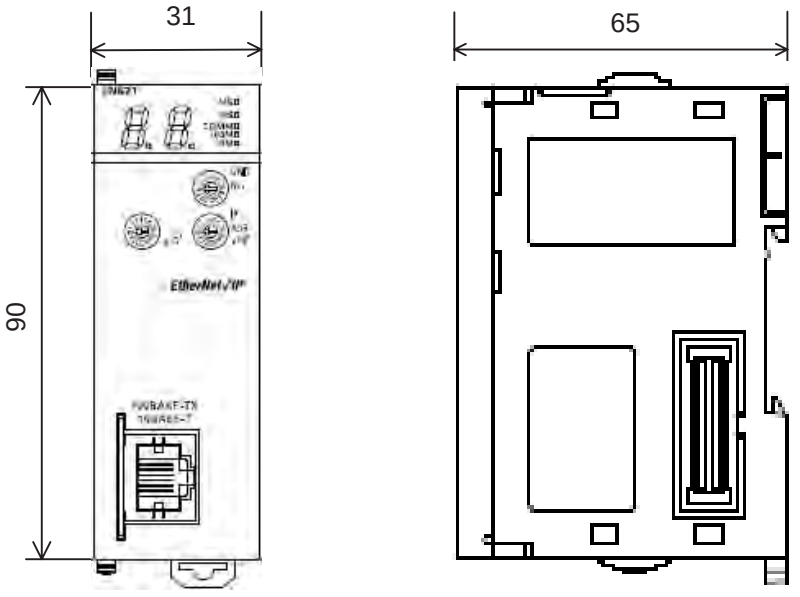
Specifications that are not listed above conform to *3-1-1 General Specifications of NE2A-series Controllers*.

Up to three EtherNet/IP Safety Units can be connected to one NE2A-series Controller. Be sure to not exceed the maximum of six Communications Units if DeviceNet Units and EtherNet/IP Units are both connected.

Note The maximum current consumption of the EtherNet/IP Safety Unit (NE2A-ENS21) is 410 mA. Mount a Power Supply Unit (NE2A-PD025) if one or more Communications Units are connected to the NE2A-series CPU Unit.

3-7-6 Dimensions (Reference Values)

Item	Specifications
Dimensions	31 × 90 × 65 mm (W × H × D)
Weight	100 g max.

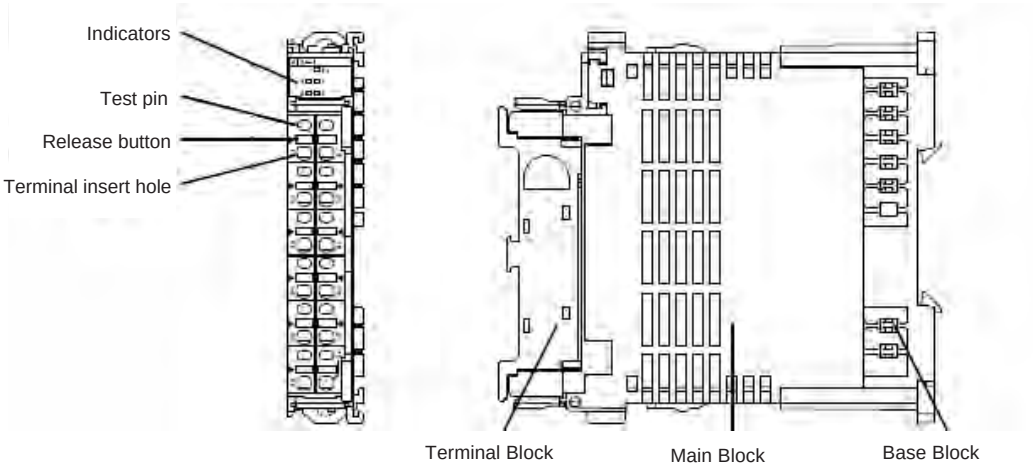


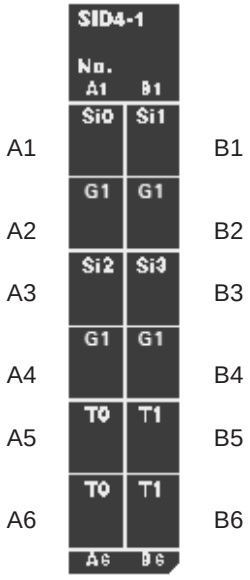
Unit: mm

3-8 Safety Input Units

3-8-1 Nomenclature and Terminal Layout

NE2A-SID4-1





3-8-2 Indicators

TS Indicator

This indicator shows the status of the Safety Input Unit.

Indicator name	Color	Status	Meaning	
TS	Green	☐	• Normal operation	
		◪	• Waiting for configuration	
	Red	☐	Error	• Unit Hardware Error Use the monitor in the Network Configurator to check the cause of the error. • CPU Unit Error
	---	■	• Unit power is not being supplied. Wire the V0 and G0 terminals on the CPU Unit (for internal control circuits) to supply power.	

☐ : ON ◪ : Flashing ■ : OFF

Input Indicators

These indicators show the status of the input terminals. Indicators 0 to 3 correspond to Si0 to Si3.

Indicator name	Color	Status	Meaning
0 to 3	Yellow	☐	• Input signal ON
	Red	☐	• Error detected in input circuit. • Discrepancy error detected when setting dual channel.
		◪	• Error detected in other channel when setting dual channels. (No error in this channel.)
	---	■	• Input signal OFF • Power for external input circuits of the Safety Input Unit is not being supplied. Wire the V1 and G1 terminals on the CPU Unit to supply power. • Discrepancy error detected when setting dual channel.

☐ : ON ◪ : Flashing ■ : OFF

3-8-3 I/O Specifications

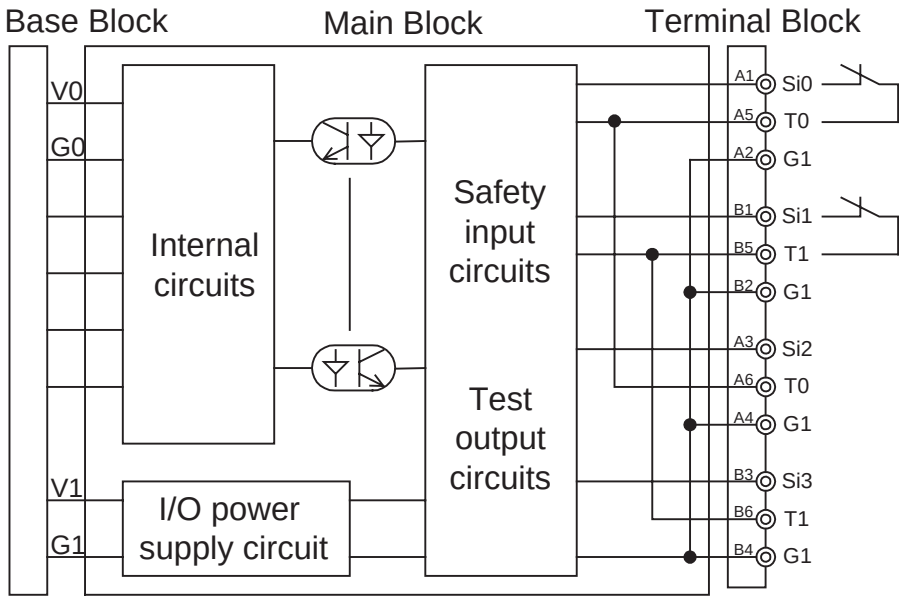
Safety Inputs

Item	Specifications
Number of inputs	4
Input type	Sinking inputs (PNP compatible)
ON voltage	11 VDC min. between input terminals and G1
OFF voltage	5 VDC max. between input terminals and G1
OFF current	1 mA max.
Input current	4.5 mA

Test Outputs

Item	Specifications
Number of outputs	2 (T0, T1)
Output type	Sourcing outputs (PNP compatible)
Rated output current	21.5 mA max.
ON residual voltage	1.2 VDC max. between output terminals and V
Leakage current	0.1 mA max.

3-8-4 I/O Terminals and Internal Connection Diagram



Terminal number	Name	Description
A1, B1, A3, B3	Si0 to Si3	Safety Input terminals
A2, B5, A6, B6	T0 to T1	Test output terminals. Use for connection to Safety Input terminals Si0 to Si3. (*1) Test output terminals T0 and T1 each outputs a different test pulse pattern. The two T0 terminals are connected internally. The two T1 terminals are also connected internally.
A2, B2, A4, B4	G1	Power supply terminals for input circuits. The four G1 terminals are connected internally.

*1 The test outputs of the Safety Input Units are independent of each other. Use the test outputs on the Safety Input Units for the Safety Inputs of those Units. An error may occur if it is used for the Safety Input of another Unit.

3-8-5 Wiring I/O Devices

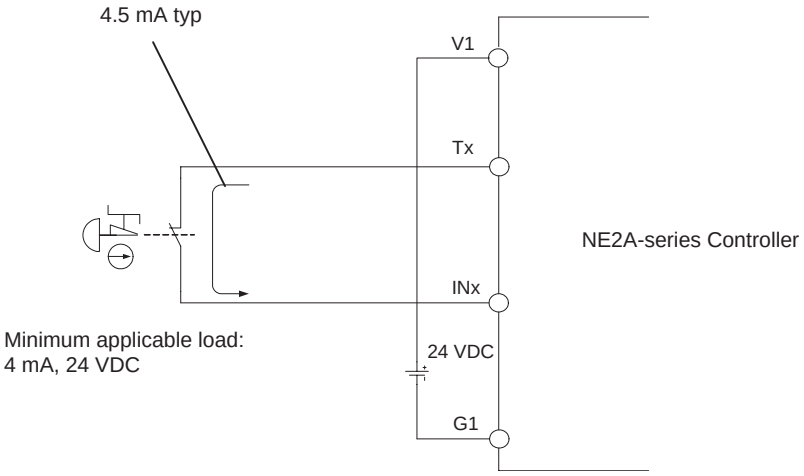
Refer to the following information for input device selection and wiring.

Devices with Mechanical Contact Outputs

Examples: Emergency stop buttons and safety limit switches

These devices use both a Safety Input terminal and test output terminal.

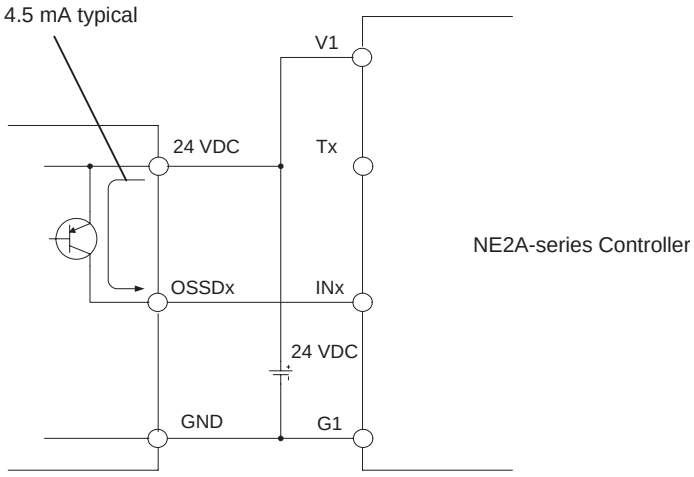
A Safety Input terminal inputs the test output signal (pulse output) of the NE2A-series Controller via a contact output device.



Devices with PNP Semiconductor Outputs (Current Sourcing)

Example: Light curtains

A PNP semiconductor output signal from this type of device is input to the NE2A-series Controller's Safety Input terminal.



⚠ WARNING

Serious injury may possibly occur due to loss of required safety functions. Use appropriate components or devices according to the requirements given in the following table.

Controlling devices	Requirements
Emergency stop switch	Use approved devices with a direct opening mechanism compliant with IEC/EN 60947-5-1.
Safety door switch or safety limit switch	Use approved devices with a direct opening mechanism compliant with IEC/EN 60947-5-1 and capable of switching micro-loads of 4 mA at 24 VDC.
Safety sensor	Use approved devices compliant with the relevant product standards, regulations, and rules in the country where they are used.

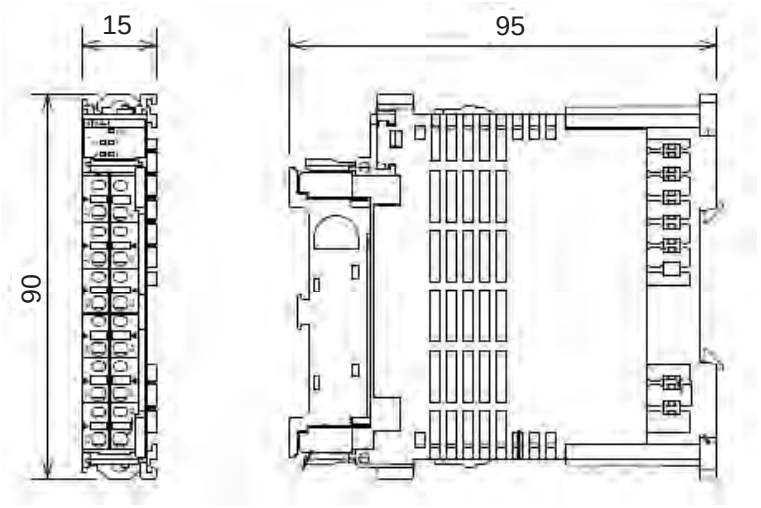
Controlling devices	Requirements
Relay with forcibly guided contacts	Use approved devices with forcibly guided contacts compliant with EN 50205. For feedback, use devices with contacts capable of switching micro-loads of 4 mA at 24 VDC.
Contactor	Use contactors with a forcibly guided mechanism and monitor the auxiliary NC contact to detect contactor failures. For feedback, use devices with contacts capable of switching micro-loads of 4 mA at 24 VDC.
Other devices	Evaluate whether devices used are appropriate to satisfy the requirements of the safety category level.

Note

- Properly apply the specified voltage to the NE1A-series Controller's inputs. Applying an inappropriate DC voltage or any AC voltage may cause reduced safety functions, damage to the NE1A-series Controller, or a fire.
- Be sure to separate I/O cables from high-voltage/current lines.
- Use I/O cables of 100 m or less.
- Do not apply the power supply to the test output terminals. Doing so may result in product damage or burning.

3-8-6 Dimensions (Reference Values)

Item	Specifications
Dimensions	15 × 90 × 95 mm (W × H × D)
Weight	90 g max.

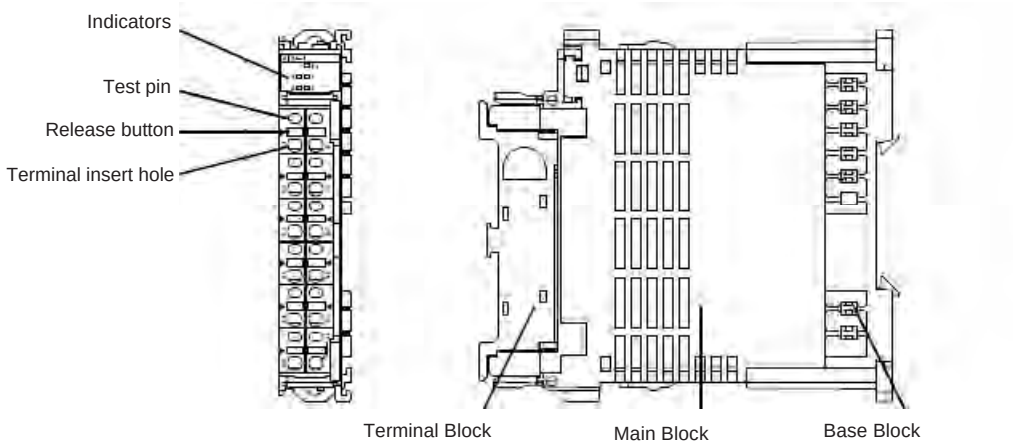


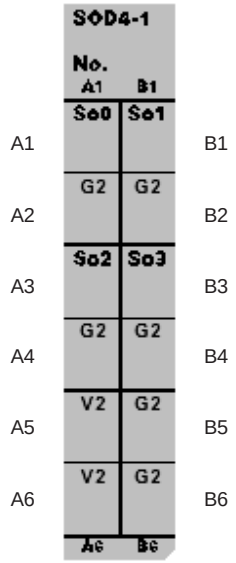
Unit: mm

3-9 Safety Output Units

3-9-1 Nomenclature and Terminal Layout

NE2A-SOD4-1





3-9-2 Indicators

TS Indicator

This indicator shows the status of the Safety Output Unit.

Indicator name	Color	Status	Meaning	
TS	Green	☐	• Normal operation	
		◪	• Waiting for configuration	
	Red	☐	Error	• Unit Hardware Error Use the monitor in the Network Configurator to check the cause of the error. • CPU Unit Error
	---	■	• Unit power is not being supplied. Wire the V0 and G0 terminals on the CPU Unit (for internal control circuits) to supply power.	

☐ : ON ◪ : Flashing ■ : OFF

Output Indicators

These indicators show the status of the output terminals. Indicators 0 to 3 correspond to So0 to So3.

Indicator name	Color	Status	Meaning
0 to 3	Yellow	☐	• Output signal ON
	Red	☐	• Error detected in output circuit. • Dual channel violation at Safety Output detected when dual channels are set.
		◪	• Error detected in other channel when setting dual channels. (No error in this channel.)
	---	■	• Output signal OFF • Power for external output circuits of the Safety Output Unit is not being supplied. Wire the power supply to V2 and G2.

☐ : ON ◪ : Flashing ■ : OFF

3-9-3 I/O Specifications

Safety Outputs

Item	Specifications
Number of outputs	4
Output type	Sourcing outputs (PNP compatible)
Power supply voltage V2	20.4 to 26.4 VDC (24 VDC –15% +10%)
Rated output current	0.5 A max./point, 1.2 A/Unit max.
ON residual voltage	1.2 VDC max. between output terminals and V2
OFF residual voltage	2 VDC max. between output terminals and G2
Leakage current	0.1 mA max.

⚠ WARNING

Outputs may fail, possibly resulting in serious injury. Never use Safety Outputs for loads that exceed the ratings. Ground faults are detected for Safety Outputs from the NE2A, but overcurrents are not detected. Make sure that the output current is within the rating.

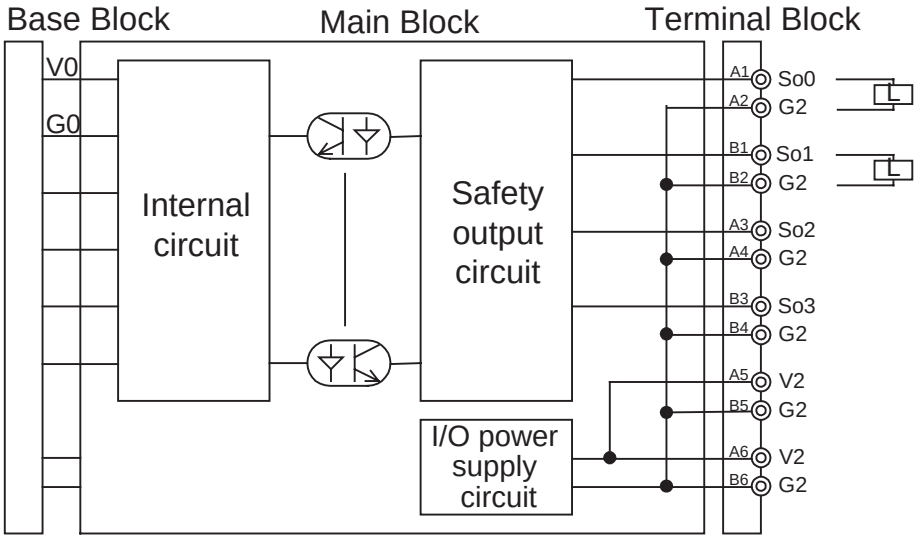


Note If a safety pulse test is set, an OFF pulse signal (pulse width: 640 us) will be output due to output circuit diagnosis when the Safety Output is ON. Be careful of the input response time of the control devices to be connected so as not to cause incorrect operation due to this OFF pulse.

Output Circuit Power Supply

Item	Specifications
Power supply voltage	20.4 to 26.4 VDC
Current capacity	1.2 A/Unit

3-9-4 Output Terminals and Internal Connection Diagram



Terminal number	Name	Description
A1, B1, A3, B3	So0 to So3	Safety Output terminals
A2, B2, A4, B4	G2	
A5, A6	V2	Power supply terminals for output circuits
B5, B6	G2	

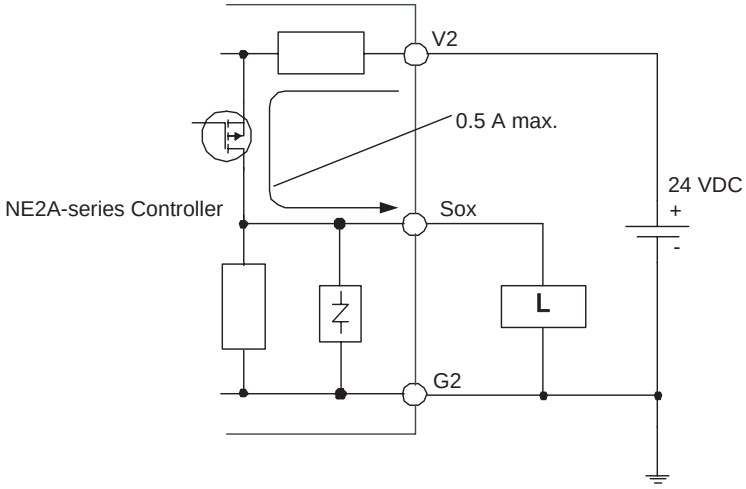
The V2 terminals (A5 and A6) are connected internally.

The G2 terminals (A2, A4, B2, B4, B5, and B6) are connected internally.

3-9-5 Power Supply Terminal Wiring and Wiring I/O Terminals

Refer to *16-2-2 Applicable Wire Sizes, Crimp Terminals, and Tightening Torque* for information on wire sizes, recommended materials, and tools.

Refer the following figure to connect output devices.



⚠ WARNING	
Serious injury may possibly occur due to breakdown of Safety Outputs or test outputs. Do not connect loads beyond the rated value to the Safety Outputs and test outputs.	
Serious injury may possibly occur due to loss of required safety functions. Wire the NE2A-series Controller properly so that the 24-VDC line does NOT touch the outputs accidentally or unintentionally and cause the load to turn ON due to shorting of the 24-VDC line.	
Serious injury may possibly occur due to loss of required safety functions. Ground the 0-V line of the power supply for external output devices so that the devices do NOT turn ON when the Safety Output line or the test output line is grounded.	
Serious injury may possibly occur due to loss of required safety functions. Use appropriate components or devices according to the requirements given in the following table.	

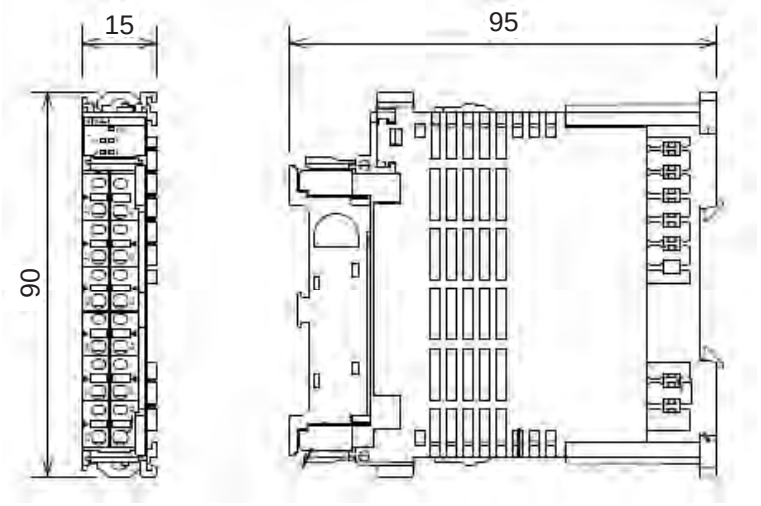
Control device	Requirements
Contactor	Use contactors with a forcibly guided mechanism and monitor the auxiliary NC contacts to detect contactor failures. For feedback signals, use devices with contacts capable of switching microloads of 4 mA at 24 VDC.
Other devices	Evaluate whether devices used are appropriate to satisfy the requirements of the safety category level.

Note

- Separate I/O cables from high-voltage lines and power lines.
- Use I/O cables of 100 m or less.
- Do not apply power to the output terminals. Doing so may result in product damage or burning.

3-9-6 Dimensions (Reference Values)

Item	Specifications
Dimensions	15 × 90 × 95 mm (W × H × D)
Weight	95 g max.



Unit: mm

SECTION 4
Status Transitions and Program Design

This section describes the operating modes and other status of the NE2A-series Safety Network Controllers and describes programming the NE2A-series Safety Network Controllers.

4-1 NE2A-series Controller Status Transitions 68
4-1-1 Operating Modes and Confirmation Methods 68
4-1-2 Moving between Operating Modes 69
4-1-3 Functions Supported in Each Operating Mode 70
4-1-4 Force-setting and Force-resetting Variables 71
4-2 Setting the Operation for Resetting and Starting 73
4-2-1 Resetting 73
4-2-2 Setting NE2A-series Operation at Startup 75
4-3 Creating Variables 76
4-3-1 Types and Uses of Variables 76
4-3-2 Linking I/O Tags to Local I/O and Remote I/O 78
4-3-3 Creating Variables 79
4-4 Creating Programs 84
4-4-1 Structured Design 84
4-4-2 Programming Using Function Blocks 84
4-4-3 Creating Library Objects and Reusing Programming 85
4-5 Checking Programming 87
4-6 Function Blocks 88

4-1 NE2A-series Controller Status Transitions

4-1-1 Operating Modes and Confirmation Methods

The NE2A-series Controller supports the operating modes shown in the following table. Synchronize these operating modes with those of other Safety Controllers and Standard PLCs.

When performing maintenance, the operating mode can be checked on the MS indicator on the front panel of the NE2A-series Controller, or by monitoring the NE2A-series Controller from the Network Configurator.

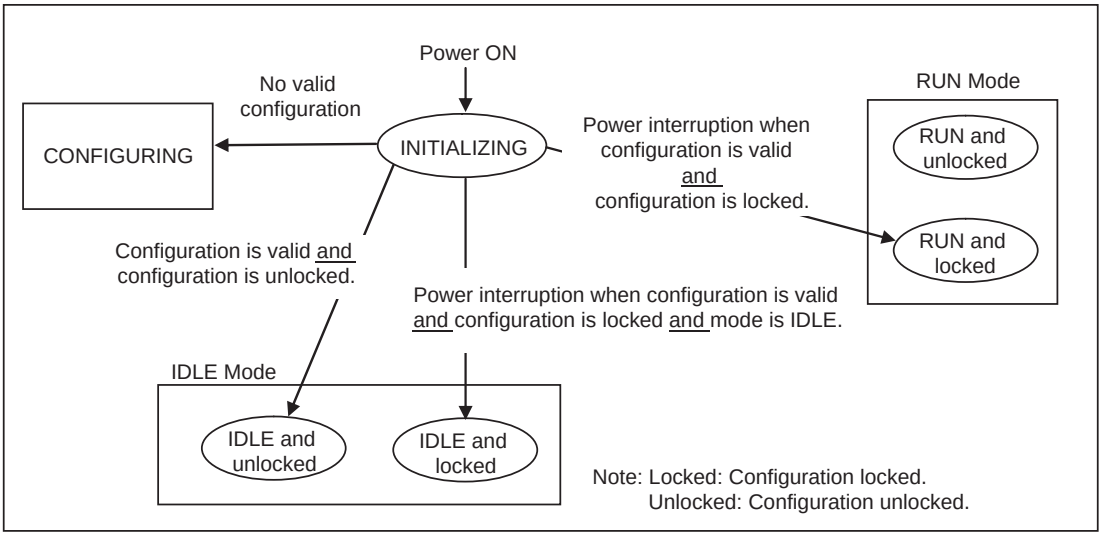
Operating mode	Description	MS indicator status	
		Color	Status
RUN Mode	In this status, both safety controls (user program execution, safety I/O communications, and local safety I/O) and non-safety controls (e.g., standard I/O communications and message communications) can be executed.	Green	☐
IDLE Mode	Configuration has been completed normally, initialization as been completed, and all the safety functions are in the following status. • The user program is stopped. • Local safety outputs are OFF. • Safety I/O communications are stopped. The standard I/O communications for the Communications Units mounted to the CPU Unit will also be stopped. In this status, only message communications are possible.	Green	◪
CONFIGURING Mode	The Controller is waiting for the configuration to be downloaded. This status is entered after initialization has been completed if the NE2A-series Controller is not configured or if there is an error in the configuration data.	Green/ Red	◪
CONFIGURATION RESTORE Mode *1	The configuration is being restored. The configuration can be downloaded and locked using a Memory Card. This mode will start once the power supply is turned ON after the function setting switch has been set. It is not possible to enter other operating modes from this mode. To change the mode, it is necessary to reset the function setting switch and restart the NE2A-series Controller.		
ABORT Mode	A non-fatal error (I/O Unit or Communications Unit configuration error) has occurred. The safety functions will go into the following safe states. • The user program will be stopped. • Local Safety Outputs will turn OFF. • Safety I/O Communications will stop. In addition, Standard I/O Communications will stop for Communications Units mounted to the CPU Unit, and only message communications will be possible.	Red	◪
CRITICAL FAULT Mode	A fatal error (hardware failure or assert error) has occurred. The safety functions will go into the following safe states. • The user logic program will be stopped. • Local Safety Outputs will turn OFF. • Safety I/O Communications will stop. In addition, Standard I/O Communications and message communications will stop for Communications Units mounted to the CPU Unit, and only message communications from the USB port will be possible.	Red	☐
INITIALIZING Mode	The self-diagnosis required to ensure safety functions is being performed.	Green/ Red	◪

☐ : Lit ◪ : Flashing ■ : Not lit

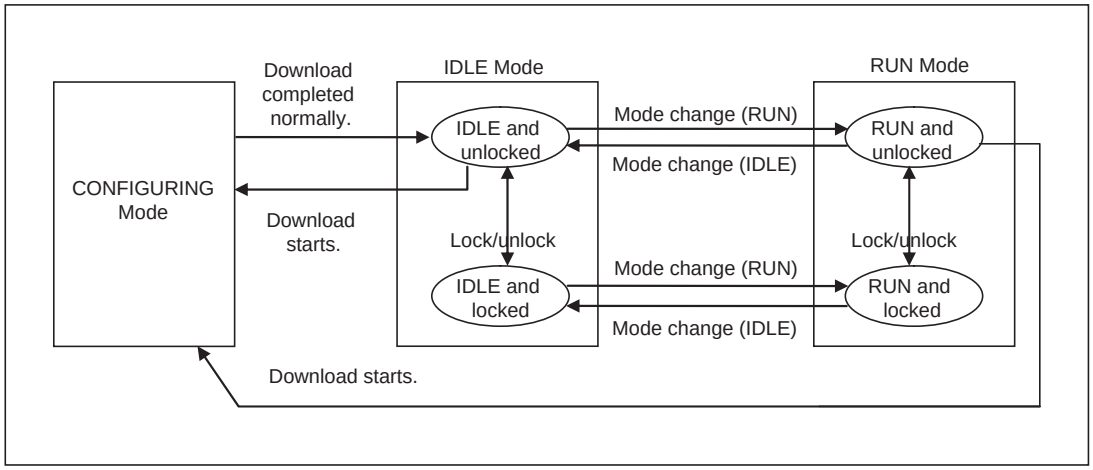
*1 For details on the CONFIGURATION RESTORE Mode, refer to *7-2 Operation and Maintenance Using a Memory Card*.

4-1-2 Moving between Operating Modes

The following diagram shows the mode changes after initialization is completed at startup.



The following diagram shows the mode changes between the RUN, IDLE, and CONFIGURING Modes.



4-1-3 Functions Supported in Each Operating Mode

The following table shows the status of each NE2A-series Controller operating mode, and the operations that are supported from the Network Configurator in each mode.

<table>
<tr><th rowspan="2">Operating mode</th><th colspan="3">Safety functions</th><th colspan="2">Standard functions</th><th colspan="6">Operations from Network Configurator</th></tr>
<tr><th>Program</th><th>Safety I/O Communications</th><th>Local I/O controls (including test output terminals)</th><th>Standard I/O Communications</th><th>Message communications</th><th>Configuration download</th><th>Configuration lock/unlock</th><th>Reset</th><th>Password changes</th><th>Online monitoring</th><th>Force-setting/resetting variables</th></tr>
<tr><td>RUN Mode</td><td>Executed</td><td>Supported (See note 4.)</td><td>I/O refreshed (See note 1.)</td><td>Supported</td><td>Supported</td><td>Supported</td><td>Supported</td><td>Supported (See note 4.)</td><td>Supported</td><td>Supported</td><td>Supported (See note 5.)</td></tr>
<tr><td>IDLE Mode</td><td>Stopped</td><td rowspan="6">Stopped</td><td rowspan="6">Safe state (See note 2.)</td><td rowspan="6">Stopped</td><td rowspan="5">Stopped</td><td rowspan="3">Not supported</td><td>Not supported</td><td rowspan="5">Not supported</td><td rowspan="3">Not supported</td><td rowspan="5">Not supported</td></tr>
<tr><td>CONFIGURING Mode</td><td rowspan="4">Not supported</td></tr>
<tr><td>CONFIGURATION RESTORE Mode</td><td>Supported (See note 3.)</td><td>Supported (See note 5.)</td></tr>
<tr><td>ABORT Mode</td><td>Not supported</td><td>Supported</td><td>Supported</td></tr>
<tr><td>CRITICAL FAULT Mode</td><td>Not supported</td><td>Not supported</td><td>Not supported</td><td>Not supported</td></tr>
<tr><td>INITIALIZING Mode</td><td>Not supported</td><td>Not supported</td><td>Not supported</td><td>Not supported</td></tr>
</table>

Note

(1) Local I/O are OFF in IDLE mode.

(2) The safe state means the following:

- Local safety outputs are OFF.
- Safety I/O communications data is OFF.

(3) The configuration can be downloaded and locked only from the NE2A CPU Unit, not by using the Network Configurator.

(4) Whether resetting is possible depends on the reset type and on the configuration settings. For details, refer to *4-2-1 Resetting*.

(5) Force-set/reset can be performed only when the configuration data is unlocked. ON can be output by force-setting local safety I/O in IDLE mode.

Variable Status during Program Execution

The following table shows the values of the variables while the program is being executed and while it is stopped.

Variable type	Program being executed	Program stopped
Input variables	Most recent input value	Most recent input value
Output variables	Program execution result	OFF
Internal variables	Program execution result	OFF

4-1-4 Force-setting and Force-resetting Variables

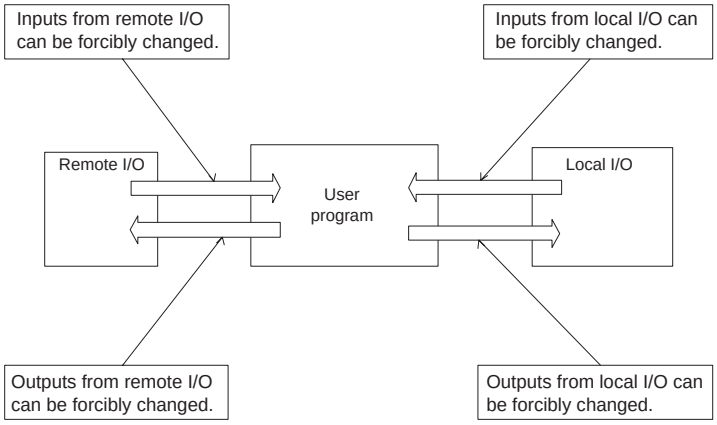
Variables to which local I/O or remote I/O have been assigned can be force-set/reset from the Safety Program Monitoring Window. Force-setting or force-resetting variables enables the values used by the program to be turned ON and OFF regardless of the ON/OFF status of the actual local I/O and remote I/O data.

Force-setting and force-resetting variables make it possible to efficiently check output wiring and debug when setting up the system.

⚠ WARNING

Outputs may operate, possibly resulting in serious injury. Real I/O may be changed directly or indirectly for any of the following. Take sufficient safety precautions.

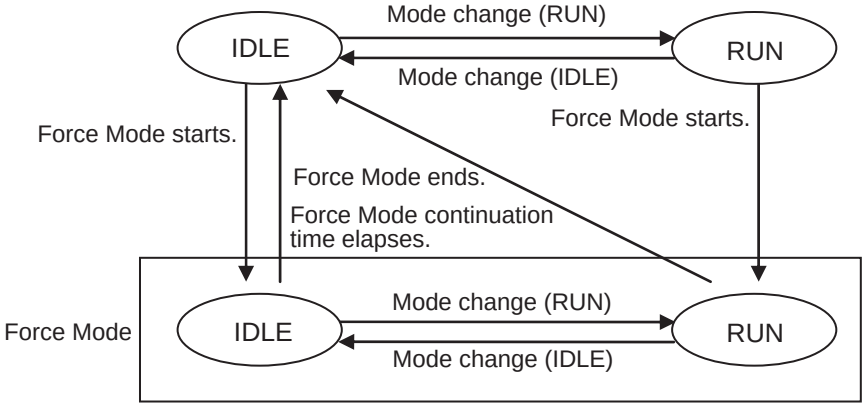
- Force-setting/resetting variables
- Ending Force Mode when the duration time expires
- Ending Force Mode from the Network Configurator



Force Mode

To force-set or force-reset variables to which inputs or outputs are assigned, the NE2A-series Controller must be changed to Force Mode.

To change to Force Mode, you must input a device password. The configuration data must be locked to change the NE2A-series Controller to Force Mode.



Monitoring Force Mode Time

There is a limit to the time that the NE2A-series Controller can continue in Force Mode. The duration time is specified when Force Mode is started or restarted. The upper limit of the duration time is 24 hours. If this time elapses, the NE2A-series Controller will exit Force Mode and move to IDLE Mode in the normal operating mode.

Note After the duration time elapses, the data that was force-set or force-reset will return to the actual I/O values. Be sure to take sufficient safety precautions.

Data That Can be Force-set/reset

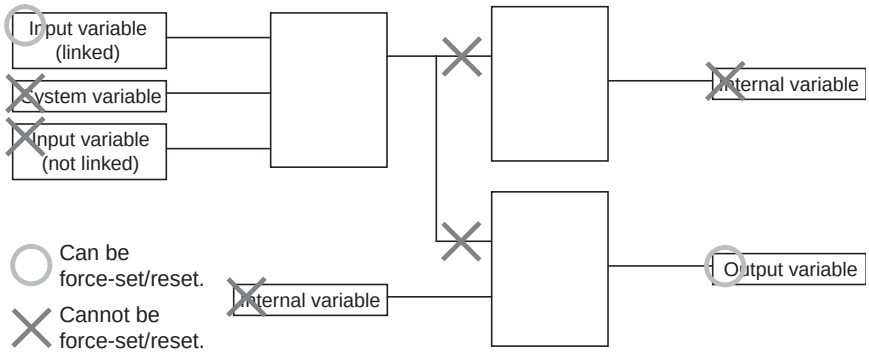
The following data can be force-set/reset.

- Input variables linked to I/O tags (local inputs, remote inputs, status)
- Input variables assigned to assemblies
- Output variables linked to I/O tags (local outputs, remote outputs, software switches)
- Output variables linked to assemblies

The following data cannot be force-set/reset.

- Input variables not linked to I/O tags or assemblies
- Output variables not linked to I/O tags or assemblies
- Internal variables (including connection signals between function blocks)
- System variables
- Remote I/O data
- Local I/O data
- Status

Signals set for dual channels can be force-set or force-reset as dual channels according to their equivalent/ complementary setting. In addition, when variables linked to EDM outputs are force-set/reset, the feedback signals will also changed.



4-2 Setting the Operation for Resetting and Starting

This section describes the settings for NE2A-series Controller operation for reconfiguration, restarting, and execution.

4-2-1 Resetting

There are three ways to reset a Safety Device.

Reset type	Description
Restart	Resets in the same way as cycling the power. (The configuration data is left unchanged.)
Restore default settings and then restart	Restores all configuration information stored in the device nonvolatile memory to the default settings, and then restarts.
Restore default settings except for specified variables and then restart	Restores all configuration information stored in the device nonvolatile memory to the default settings, except for specified information, and then restarts. The following information can be specified. • TUNID • Device password • CFUNID • OCPUNID

Safety Devices save the following configuration information in their internal non-volatile memory. Once this information is set, it is not cleared by cycling the power. To clear this information, perform the procedure for restoring the default settings and restarting. For details on this procedure, refer to *17-8 Resetting Devices*.

Type	Default setting	Set when	Description
Device parameter	Not configured	Parameters are downloaded.	Parameters and programs set by the user
TUNID (Target Unique Network Identifier)	Not set	First time parameters are downloaded.	The identifier of the local node in the Safety Network as well as the combined values of the network number and node address
Device password	No password	Password is changed.	Device password
CFUNID (Configuration Owning UNID)	Not set	First time parameters are downloaded.	UNID of the configuration source
OCPUNID (Output Connection Point Owning UNID)	Not set	Start of first safety communications	UNID of the Safety Master that opens a Safety Output configuration

Resetting DeviceNet Units

There are two types of resets for DeviceNet Units, as shown in the following table.

Reset type	Description
Restart	Resets in the same way as cycling the power. (The configuration data is left unchanged.)
Restore default settings and then restart	Restores all configuration information stored in the device nonvolatile memory to the default settings, and then restarts.

The DeviceNet Unit saves the following settings in nonvolatile memory inside the Unit. Once these settings have been made, they are not cleared when the power supply is cycled. To clear these settings and return them to the default values, select the *Return to the out-of-box configuration, and then emulate cycling power* Option when resetting. Refer to *17-8 Resetting Devices* for the procedure.

Type	Default setting	Set when	Description
Device parameter	Not configured	Parameters are downloaded.	These parameters are set by the user.

Resetting EtherNet/IP Units

There are two types of resets for EtherNet/IP Units, as shown in the following table.

Reset type	Description
Restart	Resets in the same way as cycling the power. (The configuration data is left unchanged.)
Restore default settings and then restart	Restores all configuration information stored in the device nonvolatile memory to the default settings, and then restarts.

The EtherNet/IP Unit saves the following settings in nonvolatile memory inside the Unit. Once these settings have been made, they are not cleared when the power supply is cycled. To clear these settings and return them to the default values, select the *Return to the out-of-box configuration, and then emulate cycling power* Option when resetting. Refer to *17-8 Resetting Devices* for the procedure.

Type	Default setting	Set when	Description
Device parameter	Not configured	Parameters are downloaded.	These parameters are set by the user.
TCP/IP settings	Default values*1	When the settings are made in the Unit using the Setup TCP/IP Configuration Menu Command.	IP address and subnet mask

*1 Refer to *5-2-3 EtherNet/IP Communications*.

Note

(1) When using the *Return to the out-of-box configuration, and then emulate cycling power* Option to reset the CPU Unit, use the same option to reset the Communications Unit.

(2) Do not use the *Return to the out-of-box configuration, and then emulate cycling power* Option to reset only the Communications Unit. A fatal error (abort) will occur in the CPU Unit.

4-2-2 Setting NE2A-series Operation at Startup

Setting the Program Execution Delay

When the NE2A-series Controller is started or when the mode is changed, it takes time from when the valid input values via Safety I/O Communications (i.e., the input values sent from the remote communicating devices) are updated in the input variables. If program execution is started during this interval, the initial input variable values (OFF) will be input in the program and a logic error (e.g., an EDM feedback error or a NO/NC discrepancy error) will occur in the function block. For that reason, the NE2A-series Controller supports delaying a program execution.

Program Execution Delay	Description
Disable (Execute the program without waiting for the Safety I/O Communications to start.)	The program will be executed without waiting for communications to start. The Slave input signals will not be updated in the program until communications start. (Input values will be OFF.) Program operation results will not be output to the Slaves.
Enable (Wait for the Safety I/O Communications to start before executing the program.)	Waits for all Safety I/O Communications to start and then executes the program. The start of program execution is delayed in comparison to when Disable is selected.

NE2A-series Controller Operation When Program Execution Is Delayed

Program execution will be delayed and the NE2A-series Controller will be in RUN Mode. Therefore, the program will not be executed, but local I/O and Standard Remote I/O will be refreshed.

- Input data will be updated in the internal memory of the NE2A-series Controller.
- Calculations will not be performed, so the output data will be OFF.
- The data sent in I/O communications will be IDLE data, so it will not be treated as valid data by the receiving devices.

Program Execution Conditions

Program execution will start when any one of the following conditions is satisfied after the Controller moves to RUN Mode.

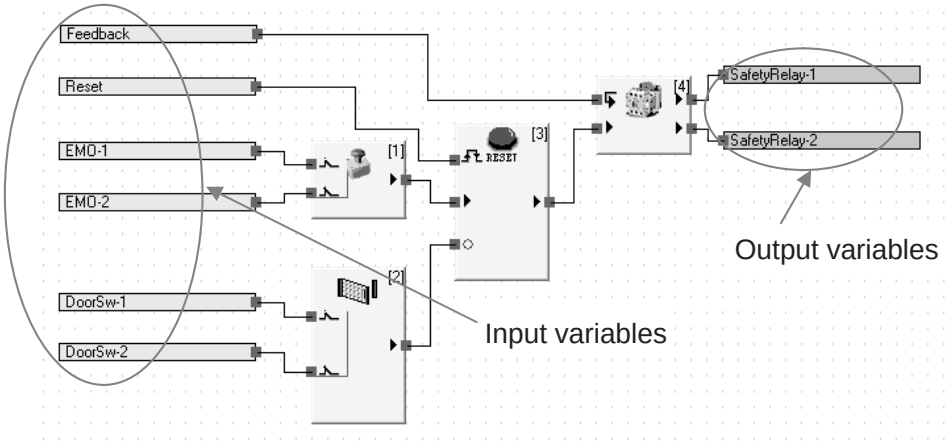
- All of the CIP safety connections that were set for the Safety Master are established.
- The program execution delay that was set has elapsed.

The program execution delay can be set from 10 ms to 200 s (in units of 1 ms). The default time is 20 ms.

4-3 Creating Variables

4-3-1 Types and Uses of Variables

Variables are used in place of device I/O tags in NE2A-series programming.



Using variables provides the following programming advantages and improves program reusability.

- Programming is possible without having to consider whether Safety I/O devices are connected to NE2A-series Safety I/O Units or to Slaves on the network.
- Once a program has been created, it does not have to be changed when the system configuration is changed.

Types of Variables

The following table shows the types of variables that can be used.

Type	Description
Input variables	Variables that can be linked to local inputs, remote inputs, and status. Variables that can be assigned to reception assembly.
Output variables	Variables that can be linked to local outputs and remote outputs. Variables that can be assigned to transmission assembly.
Internal variables	Variables that can be used only in the program. Internal variables cannot be linked to local I/O, remote I/O, or status, or assigned to assembly.
System input variables	Variables with specific functions assigned in advance. The names of the system input variables cannot be changed and the system input variables cannot be deleted. • Always ON. • Always OFF. • ON for one cycle at operation startup.

Note NE1A-series Controllers use jump addresses to pass data between function blocks, the NE2A-series Controllers use internal variables.

Differences between NE1A-series I/O Tags and NE2A-series Variables

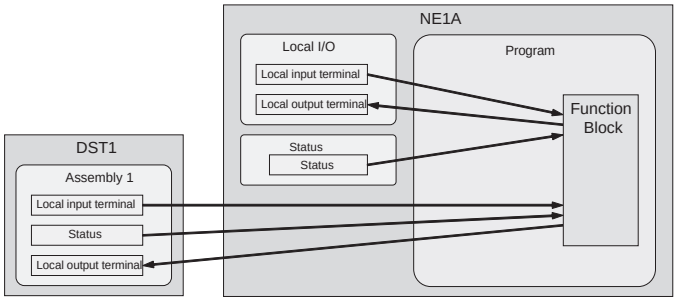
I/O tags for NE1A-series Controllers indicate local I/O terminals, remote I/O (assemblies), and status. I/O tags can be used in the program as if performing I/O directly with the terminal or assembly. Although the method is intuitive, the programming cannot be separated from the I/O terminals (assemblies) and status, and so the degree of reusability is low.

In contrast, variables with NE2A-series Controllers are separate from the I/O terminals (assemblies) and status. The I/O terminals (assemblies) and status are associated with the variables so that the I/O can be reflected in the variables themselves. This greatly improves reusability of programming.

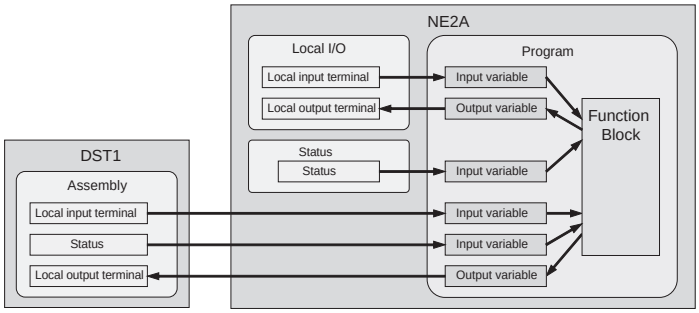
When actually programming, variables can be automatically defined by using the same procedure as with the NE1A-series Controllers, allowing direct manipulation of I/O terminals.

No	Item	NE1A-series I/O tags	NE2A-series variables
1	Name in the Program Editor	I/O tags	Input variables, output variables, and internal variables
		Jump addresses	Internal variables
2	Using remote I/O	An I/O tag cannot be used unless the connection settings are made first.	Programming can be performed with the input variables or output variables defined first. Remote I/O can be assigned afterward.
3	Effect when a connection assigned to remote I/O in operation is deleted	I/O tags in the program are deleted.	The input variable or output variable will be assigned and not defined, but there is no direct effect on the program.
4	Effect when the name (I/O comment) of a local I/O terminal or remote I/O terminal in operation is changed	The I/O tag name in the program will be automatically changed.	The variable name is not automatically changed. It must be changed by the user.

Relation between I/O Tags and the Program in the NE1A-series Controller



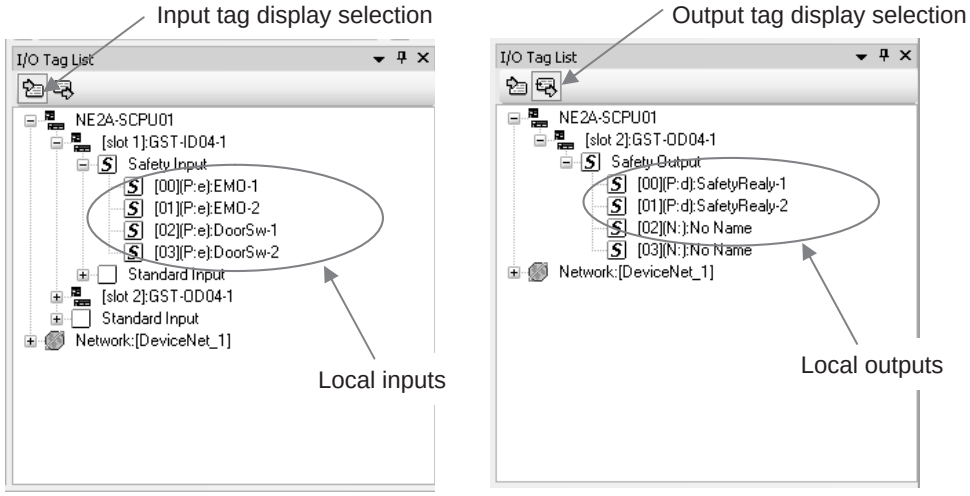
Relation between Variables and the Program in the NE2A-series Controller



4-3-2 Linking I/O Tags to Local I/O and Remote I/O

Linking I/O Tags to Local I/O

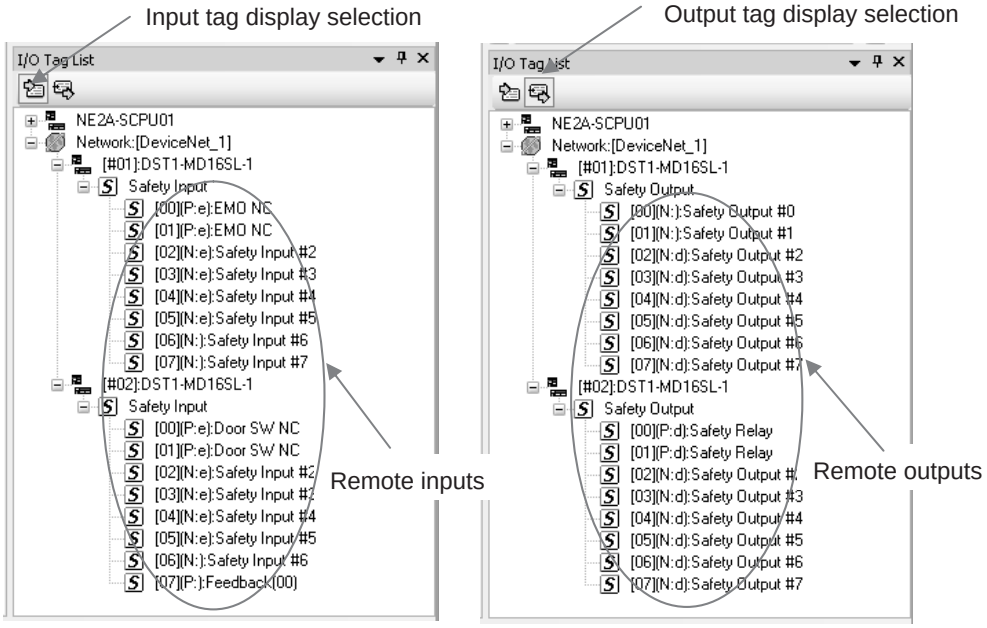
Signals, such as emergency stop, safety door, and contactor signals, connected to NE2A-series Safety I/O Units are called local I/O.
When the I/O configuration for the Safety I/O Units is set, the local I/O that is set will be displayed in the I/O Tag List as I/O tags for each Safety I/O Unit in the Logic Editor.



Linking I/O Tags to Remote I/O

Signals, such as emergency stop, safety door, and contactor signals, connected to remote communicating Slaves are called remote I/O.
NE2A-series Controllers exchange remote I/O data. To achieve this, connections must be set between the Master (NE2A) and Slaves (such as DST1).

When the NE2A-series Controller and Slave configuration is set, the remote I/O that is set will be displayed in the I/O Tag List as I/O tags for Logic Editor Slaves.

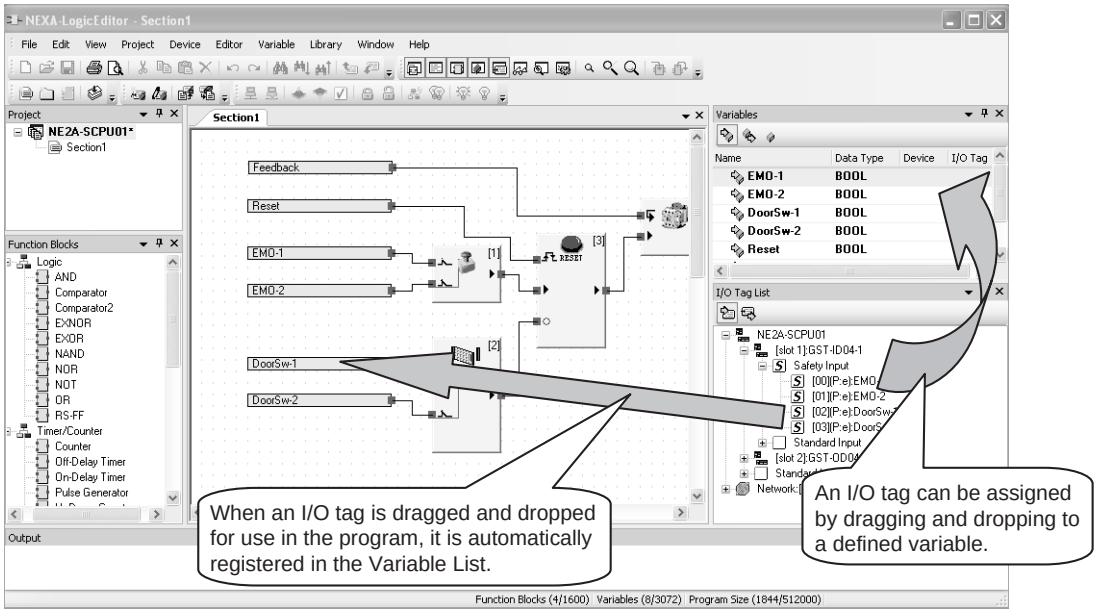


4-3-3 Creating Variables

There are two ways to create variables, as shown below.

User Definition

Specify the variable type, name, and data type.
When input or output variables are defined with this method, the variables are not linked with I/O tags. Therefore, after defining the variables, they must be linked with local I/O, remote I/O, or status, or assigned to an assembly.



Automatic Definition

Drag and drop local I/O, remote I/O, and status entities from the I/O Tag List to the Programming Pane. When an entity is dropped in the Programming Pane, a variable linked to the I/O tag will be created in the Variable List.
With this method, local I/O names (I/O comments), remote I/O names (assemblies), and status names are used as variable names.

- Rules for Automatically Created Variable Names

  Tag name _(Bit)_(Node)_(Network name)

  For local networks, variable names are created from nodes. Restricted characters are converted to underscores.

  Example:

  Local I/O and status → Tag1_00_01

  DeviceNet Safety I/O and Standard Remote I/O → Tag2_00_02_DeviceNet_1

  EtherNet/IP Safety I/O and Standard Remote I/O → Tag3_08_EtherNet_IP_192_168_250_1

  If more than 48 bytes are used, the last four characters (serial numbers from _000 to _000) will be omitted.

  TagNameAAAAAAAAAAAAAAAAAAAA_01_00_DeviceNet__000

  TagNameAAAAAAAAAAAAAAAAAAAA_01_00_DeviceNet__001

  TagNameAAAAAAAAAAAAAAAAAAAA_01_00_DeviceNet__002

  If a variable with the same name already exists, the next number will be assigned. If 999 is exceeded, an error will occur.

Variable Specifications

The following table gives the specifications of the variables that can be used in the program.

Item	Specifications	
Number of variables that can be defined	Total: 2,048 max. (excluding system variables) If all variables are BOOL data: 2,048 If all variables are BYTE data: 256 (= 2,048/8) If all variables are WORD data: 128 (= 2,048/16) If all variables are DWORD data: 64 (= 2,048/32)	
Data types	**Name**	**Description**
	BOOL	1 byte of data consisting of one Boolean bit
	BYTE	1 byte of data consisting of eight Boolean bits
	WORD	2 bytes of data consisting of 16 Boolean bits
	DWORD	4 bytes of data consisting of 32 Boolean bit
Variable names	Up to 48 characters (48 bytes) can be used. With BYTE, WORD, and DWORD data, 48-byte names can be set for individual bits in the configuration. Names are not case sensitive when ASCII characters are used. The following characters cannot be used: ! # $ % & ' " ( ) = ~ ^ \ | ` @ { + ; * : } < , > ? / . [] Also the following cannot be used: • The first character cannot be a number. • Reserved characters	

Examples of using variable data types are shown below.

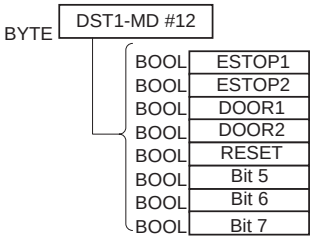
BOOL Data

In this example, the variable “ESTOP1” is set as BOOL data. It can be used as “ESTOP1” in the program.



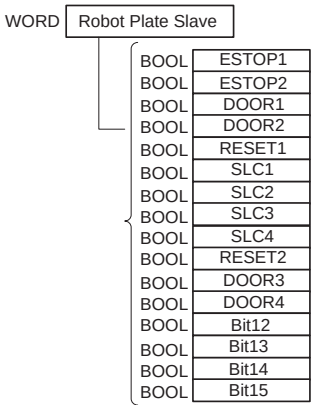
BYTE Data

In this example, the variable “DST1-MD#12” is set as BYTE data. When BYTE variables are declared, variable names can also be specified for individual bits. In the program, the first bit can be used as “DST1-MD#12. ESTOP1.”



WORD Data

In this example, the variable “Robot Plate Slave” is set as WORD data. Just as with BYTE data, variable names can also be specified for individual bits. In the program, the first bit can be used as “Robot Plate Slave. ESTOP1.”



Restrictions on Variables

For NE2A-series Controllers, information on variables cannot be accessed by using variable names from an external device, such as a PT or personal computer.

For OMRON CS/CJ-series Standard PLCs, it is possible to import variable information and I/O comment information set for I/O Terminals.

Data That Can Be Linked as Variables

With NE2A-series Controllers, the following types of data can be linked to variables and used in the program.

Data That Can Be Linked as Input Variables

Category	Data	Safety/ Non-safety	Meaning
Local I/O	Local input data	Safety	Input values for Safety Input terminals. The values after evaluation according to I/O settings.
	Local I/O status	Non-safety	Safety I/O status (evaluation result)
	Connected device maintenance status	Non-safety	Indicates whether the number of Safety I/O contact operations has exceeded the monitored threshold.
	Safety I/O Unit error status	Non-safety	Safety I/O Unit error status
Safety Remote I/O	Safety remote input data (Slaves to NE2A-series Controller)	Safety	Data received from Safety Slaves as a Safety Master
	Safety Connection normal status	Non-safety	Safety Connection (Master or Slave) communications status
	Safety Connection error status		
Standard Remote I/O	DeviceNet Master input data (Slaves to NE2A-series Controller)	Non-safety	Data received from Slaves as a DeviceNet Master
	DeviceNet Unit status 1/2	Non-safety	DeviceNet Unit status
	DeviceNet Master status	Non-safety	
	DeviceNet Slave status	Non-safety	
	DeviceNet registered Slave table	Non-safety	
	DeviceNet normal Slave table	Non-safety	
	EtherNet/IP Unit status 1/2	Non-safety	EtherNet/IP Unit status
	EtherNet/IP communications status 1/2	Non-safety	
Unit status	General status	Non-safety	Includes the various types of NE2A-series Controller status.
	Error Status	Non-safety	Includes the various types of NE2A-series Controller error information.
	Fault present	Non-safety	Indicates function block execution status and the presence of errors.

Data That Can Be Linked as Output Variables

Category	Data	Safety/ Non-safety	Meaning
Local I/O	Local output data	Safety	Values output to Safety Slice I/O Units
Safety Remote I/O	Safety remote output data (NE2A-series Controller to Slaves)	Safety	Data sent to Safety Slaves as a Safety Master
	Safety Connection communications restart software switch	Non-safety	Software switch for restarting Safety Connections (Master) stopped by communications errors
Standard Remote I/O	DeviceNet Master output data (NE2A-series Controller to Slaves)	Non-safety	Data sent to Slaves as a DeviceNet Master

Variable Data Files for Importing and Exporting

The variable data file when importing or exporting will be in CSV format. It will store the variable names, variable types (e.g., input, output, external), data types, devices, and I/O tags. (The character encoding for the output file is Shift JIS.) The CSV file uses the following format.

Line 1: Identifier and version information (#NEXA-Logic Editor Variable Export File V1.00)

Note The file will not be read if the identifier does not match.

Lines 2 or Higher:

Column 1: Name

Column 2: Variable type (VAR, VAR_INPUT, VAR_OUTPUT)

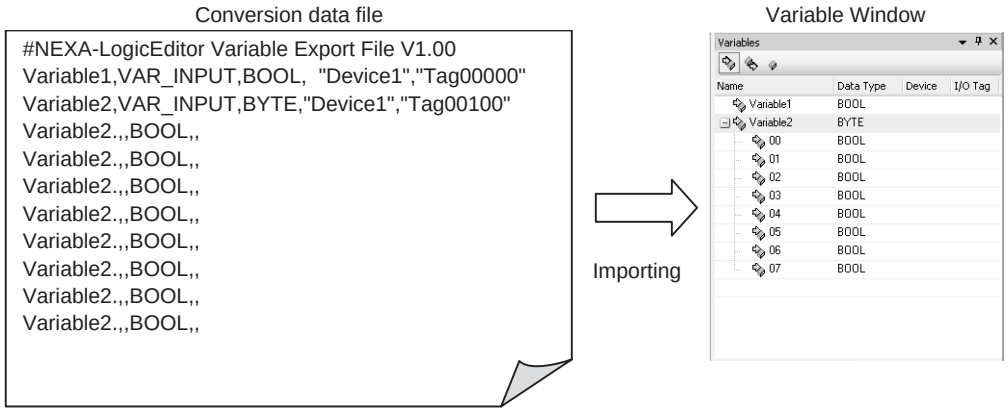
Column 3: Data type (BOOL, BYTE, WORD, DWORD)

Column 4: Device

Column 5: I/O tag

The bit members for BYTE, WORD, and DWORD data and are name and data type only. (The address indicates the continuous area starting with the parent variable.) The name is the *parent_variable_name.bit_name*. The default value will be used if there are no bit member lines or not enough bit member lines. Any line that is not preceded by a parent variable name will be ignored.

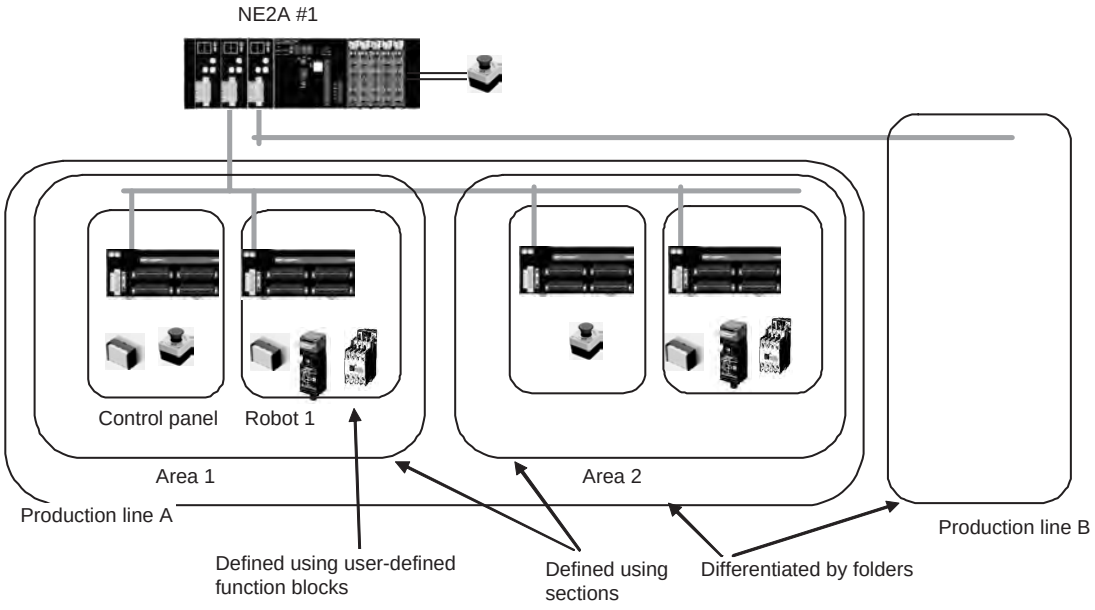
Example:



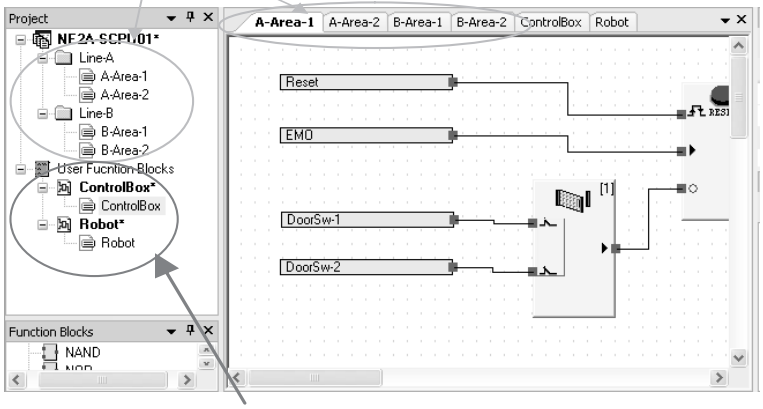
4-4 Creating Programs

4-4-1 Structured Design

Structuring a safety control system into control units, such as by production line or area, makes design more efficient and improves maintenance. With the NE2A-series Logic Editor, sections and user-defined function blocks can be used to make this type of structured design.



System designed by line or area using folders and sections.

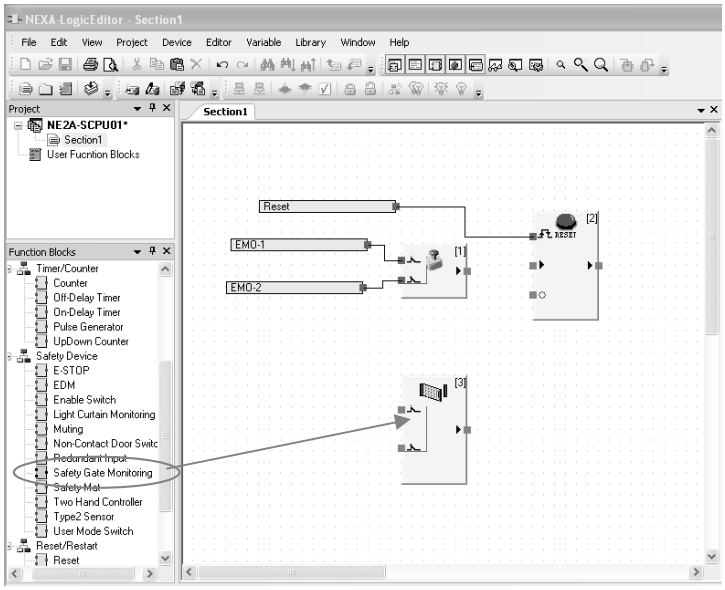


System designed by device or function using user-defined function blocks.

4-4-2 Programming Using Function Blocks

NE2A-series Controller programs are created using function blocks.
Function blocks are programming elements that determine outputs for inputs. Programming using function blocks makes safety logic easy to understand because Controllers and Safety Devices are designed using virtual components.

NE2A-series Controller programs are created by selecting from function blocks displayed in the Network Configurator function block list.



Program Size

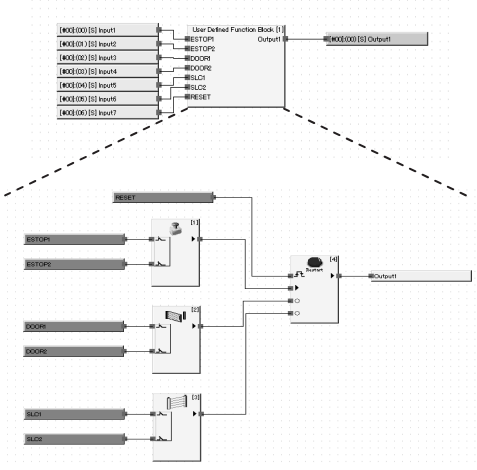
The maximum size of an NE2A-series user program is as follows:

Number of function blocks that can be used	Program size
1,600 max.	125 Ksteps (512 Kbytes)

4-4-3 Creating Library Objects and Reusing Programming

User-defined Function Blocks

You can define new function blocks by combining the function blocks that are provided by the Network Configurator.



Security can be set for a user-defined function block to prevent unauthorized personnel from accessing or changing the function block. For details, refer to *7-1 Access Control with Passwords*.

Converting Programs into Library Objects

Programs can be managed as library objects. Programs can be registered and reused in the following units.

- All or part of a program

- User-defined function blocks

When a program is registered in the library, the variables and function blocks that are being used will be registered without any changes. If the variable has an association to local I/O, remote I/O, or status, the association will be deleted and registered as an internal variable.

Importing NE1A Programs

Programs for an NE1A-series Controller can be imported into an NE2A-series Controller by using the Network Configurator. It is not possible, however, to import I/O tags from an NE1A-series Controller. After the program is imported to the NE2A-series Controller, it is necessary to allocate variables to the function block I/O and to associate the I/O tags.

4-5 Checking Programming

The programming is checked to make sure that the program that was created functions as intended. Checking the programming before checking the actual devices (downloading) reduces download errors and communications errors during execution.

The programming is checked at the following times.

- When a command is executed from a menu (performed manually).
- When a project is saved (performed automatically).
- Before downloading (performed automatically).

The following checks are performed for programs in all sections. The results of the checks are displayed in the Output Window. To display the location of a display item, double-click the display item in the Output Window.

Description	Level
Unconnected function blocks (A check is performed to find whether there are any missing connections for function blocks for the displayed inputs and outputs.)	Error
The program capacity has been exceeded.	Error
An internal variable was used only for an input or only for an output.	Warning
The same output variable is assigned more than once.	Warning

Error: The program cannot be downloaded to the NE2A-series Controller.

Warning: The program can be downloaded to the NE2A-series Controller. Check to be sure that the program is correct.

4-6 Function Blocks

Functions that are required for safety control are provided by the NE2A-series Controller in function blocks. The NE2A-series Controller supports the following function blocks, including all function blocks that are supported by the NE1A-series Controllers. For details on function block specifications, refer to the *Command Reference Manual* (Cat. No. Z920).

Function Blocks for Logic Functions

No	Function Block		Description	Compatibility
	Abbreviation	Name		
1	NOT	NOT	Outputs the logical complement of the input condition.	NE1A-compatible
2	AND	AND	Outputs the logical AND of the input conditions.	NE1A-compatible
3	OR	OR	Outputs the logical OR of the input conditions.	NE1A-compatible
4	NAND	NAND	Outputs the logical complement of the logical AND of the input conditions.	NEW
5	NOR	NOR	Outputs the logical complement of the logical OR of the input conditions.	NEW
6	EXOR	Exclusive OR	Outputs the exclusive OR of the input conditions.	NE1A-compatible
7	EXNOR	Exclusive NOR	Outputs the exclusive NOR of the input conditions.	NE1A-compatible
8	RS-FF	Reset/Set Flip-Flop	When the input turns ON, RS-FF holds the ON status in the function block and the output continues to Output Enable. When RESET is turned ON, the signal held in the function block turns OFF.	NE1A-compatible
9	Comparator	Comparator	Compares multiple signals with the comparison value set in the configuration and outputs when all the signals match the set value.	NE1A-compatible
10	Comparator2	Comparator 2	Compares multiple signals with the comparison value set in the configuration and outputs the result of the comparison.	NEW

Function Blocks for Timers and Counters

No	Function Block		Description	Compatibility
	Abbreviation	Name		
1	Counter	Counter	Counts the number of input signals and turns ON Output Enable when the count reaches the number set in the configuration data.	NE1A-compatible
2	Off-Delay Timer	Off-delay Timer	Operates an OFF-delay timer set in 10-ms units.	NE1A-compatible
3	On-Delay Timer	On-delay Timer	Operates an ON-delay timer set in 10-ms units.	NE1A-compatible
4	Pulse Generator	Pulse Generator	Cyclically outputs ON/OFF pulses while the input is ON.	NE1A-compatible
5	Up-Down Counter	Up-Down Counter	Increments the count when the incrementing counter input turns ON and decrements the count when the decrementing counter input turns ON.	NEW
6	Serial-Parallel Converter	Serial-Parallel Converter	Outputs the number of input signals as parallel signals.	NEW

Function Blocks for Safety Devices

No	Function Block		Description	Compatibility
	Abbreviation	Name		
1	EDM	External Device Monitoring	Combines the EDM (monitors the OSSD and an NC (normally closed) external device (contactor) signal) with a reset/restart and OSSD output control.	NE1A-compatible
2	Enable Switch	Enable Switch Monitoring	Monitors the status of enable switch devices.	NE1A-compatible

No	Function Block		Description	Compatibility
	Abbreviation	Name		
3	E-STOP	Emergency Stop Switch Monitoring	Monitors the status of the emergency stop switch.	NE1A-compatible
4	Light Curtain Monitoring	Light Curtain Monitoring	Monitors a Type-4 Safety Light Curtain.	NE1A-compatible
5	Muting	Muting	Temporarily disables the light interrupted signal (AOPD input) of a light curtain when the muting signal is detected. During muting, the equipment is not stopped, and the sensing object can pass through the detection area of the light curtain.	NE1A-compatible
6	Muting Parallel	Parallel Muting with Two Sensors	Performs the same Parallel Muting with 2 Sensors operation as the Muting function block.	NEW
7	Muting Forward Direction	Sequential Muting in Forward Direction	Performs the same parallel Sequential Muting in Forward Directions operation as the Muting function block.	NEW
8	Muting Both Direction	Sequential Muting in Both Directions	Performs the same Sequential Muting in Both Directions operation as the Muting function block.	NEW
9	Muting Position Detection	Muting for Position Detection	Performs the same Position Detection operation as the Muting function block.	NEW
10	Safety Gate Monitoring	Safety Gate Monitoring	Monitors the status of a safety gate (e.g., safety door switch or safety limit switch). It is possible to set function tests that comply with safety category 2.	NE1A-compatible
11	Two Hand Controller	Two Hand Controller	Monitors Two-hand Switch status according to EN 574.	NE1A-compatible
12	User Mode Switch	User Mode Switch Monitoring	Monitors the operating mode switch for the user system or device.	NE1A-compatible
13	Redundant Input	General-purpose 2-input Switch Monitoring	General-purpose monitoring of 2 input signals equivalent to monitoring a light curtain.	NEW
14	Single Beam Safety Sensor	Single Beam Safety Sensor Monitoring	Monitors the input signal of a Single-beam Safety Sensor.	NEW
15	Non-Contact Door Switch	Non-Contact Door Switch Monitoring	Monitors an OMRON Non-contact Door Switch (D40A).	NEW
16	Safety Mat	Safety Mat Monitoring	Monitors a safety mat.	NEW

Function Blocks for Reset and Restart

No	Function Block		Description	Compatibility
	Abbreviation	Name		
1	Reset	Reset	Output is not made active as long as the function block is not reset even if the relevant output conditions are satisfied.	NE1A-compatible
2	Restart	Restart	The specifications are the same as for reset function block. The icon is different.	NE1A-compatible

Function Blocks for Connectors

No	Function Block		Description	Compatibility
	Abbreviation	Name		
1	Multi Connector	Multiconnector	Outputs input signals (8 max.) to output signals.	NE1A-compatible
2	Routing	Routing	Allocates an input signal to multiple signals.	NE1A-compatible

SECTION 5
Communications

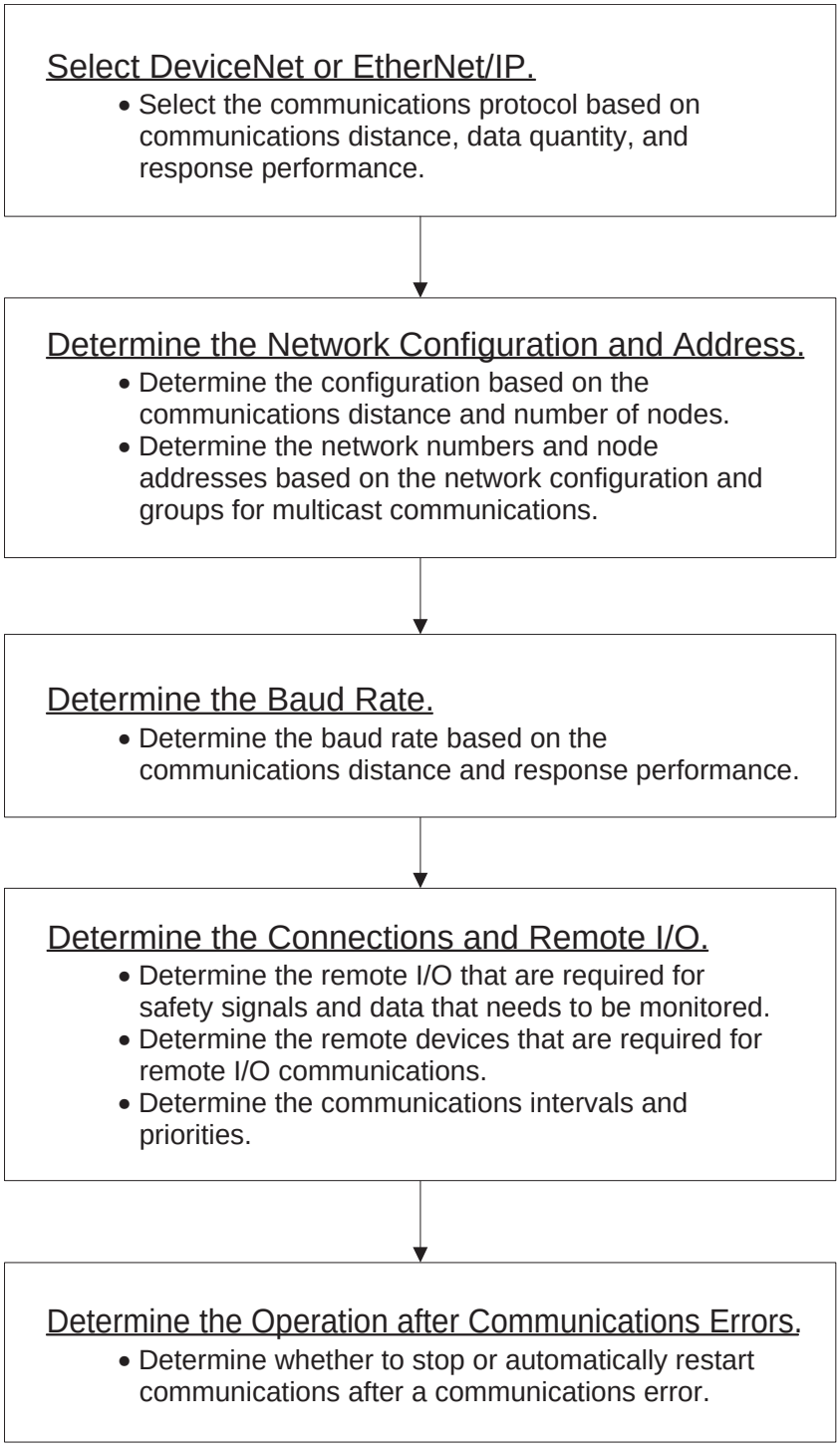
This section describes communications for the NE2A-series Safety Network Controllers.

5-1 Designing the Network System Configuration 92
5-2 Communications Specifications for NE2A-series Controllers 93
5-2-1 Connection Specifications 93
5-2-2 DeviceNet Communications 95
5-2-3 EtherNet/IP Communications 97
5-3 DeviceNet and EtherNet/IP Routing 101
5-3-1 Routing between DeviceNet and EtherNet/IP Networks 101
5-3-2 Routing with an Ethernet Switching Hub 101
5-4 DeviceNet Safety Communications 102
5-4-1 Outline of DeviceNet Safety Communications 102
5-4-2 Setting Safety Connections 102
5-5 DeviceNet Standard Communications 107
5-5-1 Outline of DeviceNet Standard Communications 107
5-5-2 Standard Connection Settings 108
5-6 EtherNet/IP Safety Communications 111
5-6-1 Outline of EtherNet/IP Safety Communications 111
5-6-2 Setting the Safety Connections 111
5-7 EtherNet/IP Standard Communications 113
5-7-1 Outline of EtherNet/IP Tag Data Link Communications 113
5-7-2 Setting Tag Data Link Connections 114
5-8 Remote I/O Allocations 121
5-8-1 Outline of Remote I/O Allocations 121
5-8-2 Configuring Assemblies 122
5-8-3 Data Elements Set in Assemblies 124
5-9 Operation after a Communications Error 136
5-9-1 Data and Operation after a Communications Error 136
5-10 Selecting the Ethernet Switching Hub 137
5-10-1 Switching Hub Types 137
5-10-2 Switching Hub Functionality 137
5-10-3 Precautions When Selecting a Switching Hub 137

5-1 Designing the Network System Configuration

This section describes DeviceNet Safety Communications, DeviceNet Standard Communications, EtherNet/IP Safety Communications, and EtherNet/IP Standard Communications that can be used with the NE2A-series Controllers.

The following points must be considered when designing the network system configuration.



5-2 Communications Specifications for NE2A-series Controllers

5-2-1 Connection Specifications

This section describes the connection specifications for NE2A-series Controllers when using DeviceNet communications and EtherNet/IP communications.

The NE2A-series Controllers perform safety communications using the DeviceNet Safety and EtherNet/IP Safety protocols. Connections are set for these two communications protocols, and they are collectively called CIP Safety Communications. CIP Safety Communications is a highly reliable safety communications system with a safety protocol added to the Common Industrial Protocol (CIP) in the network.

Item		Specifications
CIP Safety Communications connections	NE2A-series Controller (totals)	• Maximum number of connections as a Master: 160 • Maximum number of connections as a Slave: 32 • Connection types: Single Cast, Multicast
	DeviceNet Safety Unit	■ As DeviceNet Safety Master • Maximum number of connections per Unit: 64 • I/O size per connection: 16 bytes ■ As DeviceNet Safety Slave • Maximum number of connections per Unit: 4 *1 • I/O size per connection: 16 bytes
	EtherNet/IP Safety Unit	■ As EtherNet/IP Safety Master • Maximum number of connections per Unit: 128 • I/O size per connection: 32 bytes ■ As EtherNet/IP Safety Slave • Maximum number of connections per Unit: 8 • I/O size per connection: 32 bytes
DeviceNet I/O communications connections	DeviceNet Unit	■ As DeviceNet Master • Maximum number of connections per Unit: 126 • Maximum number of Slaves per Unit: 63 (2 connections per Slave) • I/O size per connection: 16 input bytes + 16 output bytes • Connection types: Poll, Bit strobe, COS, Cyclic ■ As DeviceNet Slave • Maximum number of connections per Unit: 2 • I/O size per connection: 200 input bytes + 200 output bytes (The setting cannot exceed the maximum I/O size of the DeviceNet Master) • Connection types: Poll, Bit strobe, COS, Cyclic
EtherNet/IP Tag Data Link communications connections	EtherNet/IP Unit	■ As EtherNet/IP Tag Data Link Target *2 • Maximum number of connections per Unit: 2*3 • I/O size per connection: 1,024 bytes • Connection types: Point to Point, Multicast • Connection I/O types: Input Only, Output Only, and Input & Output

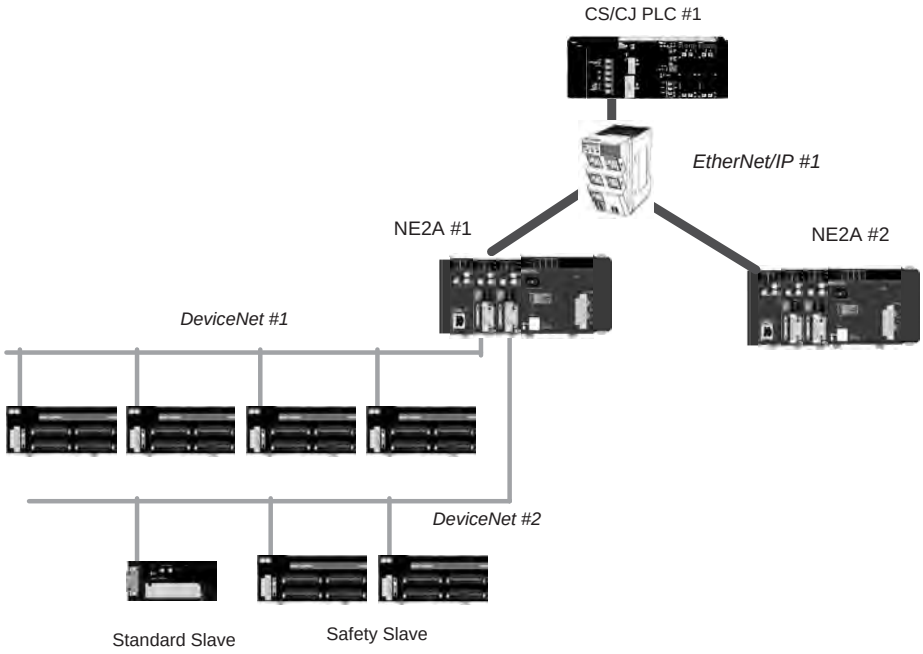
*1 With a multicast connection, input data can be sent to up to 15 Safety Masters. However, this is limited to Safety Masters that have the same I/O data type and EPI value specified for the I/O connection.

*2 Only connections as a Tag Data Link Target are supported.
The EtherNet/IP Unit cannot be an Originator.
Originator: The devices that actively establishes a connection.
Target: The device to which an connection is established.

*3 With a multicast connection, input data can be sent to up to four Originators. However, this is limited to Originators that have the same input data, packet interval (RPI), and timeout value specified for the I/O connection.

Note The NE2A-series Controllers support message communications through the DeviceNet Units and EtherNet/IP Units.

The following configuration will be used to describe the types and numbers of connections that can be set for an NE2A-series Controller.



1. Connections Set for NE2A #1

DeviceNet #1

- Safety Master: Input data and output data are set for four Slaves: 8 connections

DeviceNet #2

- Safety Master: Input data and output data are set for two Slaves: 4 connections
- Standard Master: Poll connection is set for one Slaves: 1 connection

EtherNet/IP #1

- Safety Slave: Input data and output data are set NE2A #2 (Master): 2 connections
- Tag Data Link Communications Target: An input connection and output connection are set with CS/CJ #1: 2 connections

	Safety Connections				**Standard Connections**			
	As Master	***2**	**As Slave**	***2**	**As Master**	***2**	**As Slave**	***2**
DeviceNet #1	IN: 4, OUT: 4	8/64	0	0/4	0	0/126	0	0/2
DeviceNet #2	IN: 2, OUT: 2	4/64	0	0/4	Poll: 2	2/126	0	0/2
	As Master	***2**	**As Slave**	***2**	**---**	***2**	**As Target**	***2**
EtherNet/IP #1	0	0/128	IN: 1, OUT: 1	2/8			Input&Output	2/16
Total for NE2A *1	12/160		2/32		---			

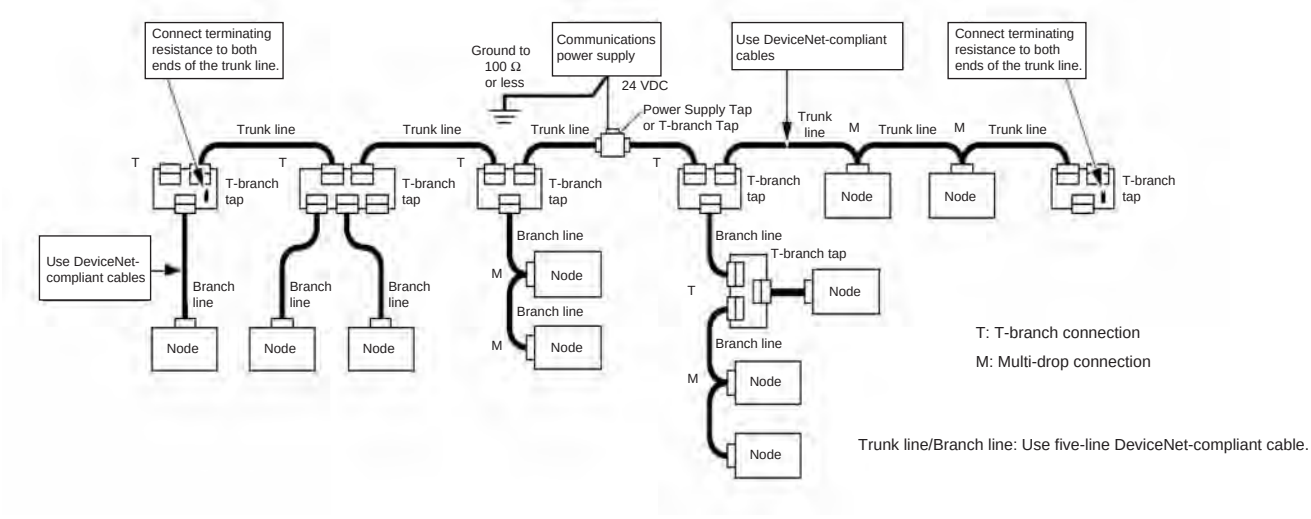
*1 Number of connections for CIP Safety Communications (set number/maximum number)

*2 Number of connections per Unit (set number/maximum number)

5-2-2 DeviceNet Communications

DeviceNet Network Configuration

The DeviceNet network configuration is shown in the following diagram.



DeviceNet Communications Specifications

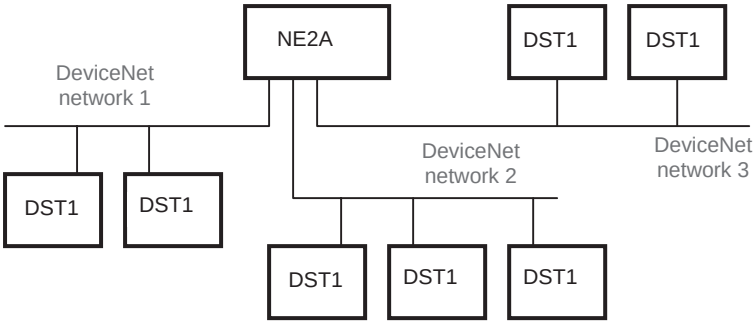
Item	Specifications			
Connection methods	Multidrop and T-branch connections can be combined for trunk line and branch lines.			
Baud rate	500 kbits/s, 250 kbits/s, or 125 kbits/s			
Communications medium	Special DeviceNet cable with 5 lines (2 communications lines, 2 power lines, 1 shield line)			
Communications distance	Baud rate	Maximum network length	Branch length	Total length
	500 kbits/s	100 m max. (100 m max.)	6 m max.	39 m max.
	250 kbits/s	250 m max. (100 m max.)	6 m max.	78 m max.
	125 kbits/s	500 m max. (100 m max.)	6 m max.	156 m max.
	The numbers in parentheses are the lengths when Thin Cable is used.			
Communications power supply	11 to 25 VDC			
Connected nodes	64 nodes max. (The total number of Standard Devices and Safety Devices that can be connected to the same network is 64. This includes the Network Configurator if it is connected.)			
Connected Slaves	63 units max.			

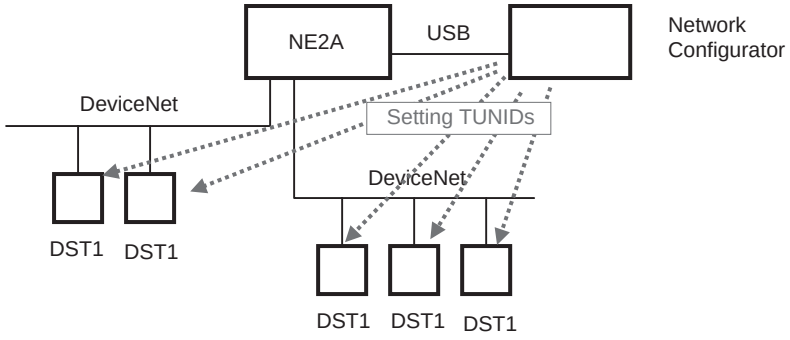
Note One NE2A-series Controller can function simultaneously as a Safety Master, Safety Slave, Standard Master, and Standard Slave.

Network Numbers and Node Addresses

Multiple DeviceNet networks can be constructed in a NE2A-series System. Network numbers are used to uniquely identify and mutually confirm the devices within a configuration containing more than one DeviceNet network, as shown in the following diagram.

To uniquely identify a device, a TUNID (Target Unique Network Identifier) that combines the network number and device node address is used.





Setting TUNIDs

The TUNID is automatically set when parameters are first downloaded from the Network Configurator to a device in out-of-the-box configuration. (See note.)

Note "Out-of-the-box configuration" indicates the status when a reset-type device is returned to its default status and restarted.

Users do not normally need to be aware of the existence of network numbers because they can visually identify a device on the Network Configurator.

The default network number is automatically generated based on the date and time the Network Configurator created the network configuration, but it can also be specified by the user.

Setting a Network Number

A network number needs to be specified in the following cases.

- When multiple Network Configurators are used to set individual devices
- When more than one Network Configurator is used to make settings on the same network, the same network number must be set for each Network Configurator.
- When more than one type of Support Software is used.

Note

(1) If the network number is not set correctly, a connection may be opened to a different device. A different network number must be set for each network domain. The same network number must be set for all the devices on the same domain.

(2) Users do not normally need to be aware of the existence of network numbers because they can visually identify devices on the Network Configurator.

Setting a Node Address

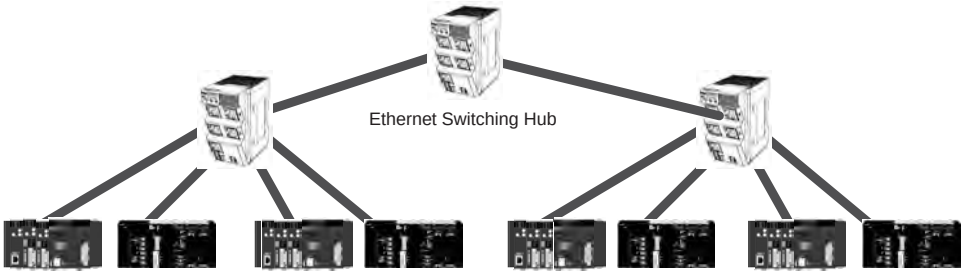
The node address can be set to any number between 00 and 63, as long as the same address is not set on another node in the same network. A node address duplication error will occur if the same address is set for more than one node. Communications will not start if this error occurs.

Set the node address of an NE2A-series DeviceNet Safety Unit (NE2A-DNS21) so that it matches the setting on the rotary switches. Refer to *3-6-3 Switches* for how to set the node address on the rotary switches.

5-2-3 EtherNet/IP Communications

EtherNet/IP Network Configuration

The EtherNet/IP network is configured as shown in the following diagram.



Ethernet Specifications

Item		Specifications	
Type		100BASE-TX	10BASE-T
Connection method		Star configuration	
Baud rate		100 Mbit/s *1	10 Mbit/s *1
Communications medium		• STP (4-pair, shielded twisted-pair) cable. • Supports categories 5 and 5e. • Impedance characteristics: 100 Ω	• STP (4-pair, shielded twisted-pair) cable. • Supports categories 3, 4, 5, and 5e. • Impedance characteristics: 100 Ω
Communications distance	Maximum cable length	100 m	
	Maximum distance between nodes	---	
	Number of cascade connections	There is no limit to the number of cascade connections if switching is performed.	

*1 Auto Negotiation (automatic setting)

Tag Data Links and Specifications

Item	Specifications
Total bandwidth	6,000 pps *2
Refresh cycle	1 to 10,000 ms (1-ms increments, default: 50 ms)
Renew cycle precision	RPI 1 to 500 ms: RPI ±15% RPI 501 ms to 1 s: RPI ±10% RPI 1.001 to 10 s: RPI ±5%

*2 “pps” means “packet per second” and indicates the number of packets that can be processed in one second. The total bandwidth is the total number of packets for both Safety I/O Communications and Tag Data Links.

Other Services

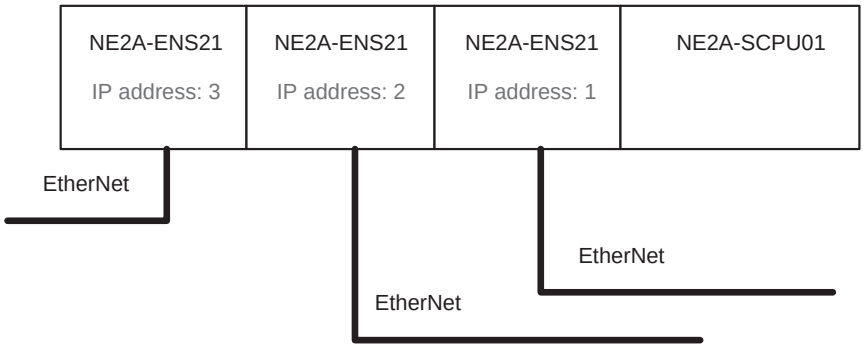
Item	Specifications
BOOTP client	IP parameters, such as the IP address and subnet mask, are automatically set for the EtherNet/IP Unit from the BOOTP server on the network.
IGMP client	When an Ethernet switch that supports IGMP snooping is used, only the necessary IP multicast packets are received. This function prevents traffic increases due to unnecessary IP multicast packets and load increases during the signal reception processing.

Setting IP Addresses (Node Addresses) and TCP/IP

Multiple EtherNet/IP networks can be constructed in a NE2A-series System.

IP addresses are used to uniquely identify and mutually confirm devices in a configuration that contains more than one EtherNet/IP (Ethernet) network.

When multiple EtherNet/IP Units are connected, as shown in the following diagram, IP addresses are used to distinguish the EtherNet/IP Units.



TCP/IP settings, such as the IP address and subnet mask, are made for an EtherNet/IP Unit.

The EtherNet/IP Unit's TCP/IP configuration settings include the following settings.

- IP address
- Subnet mask
- Default gateway
- Preferred DNS server
- Alternate DNS server
- Domain name
- Baud rate

If the NE2A-ENS21 EtherNet/IP Unit is connected to an NE2A-series CPU Unit and the TCP/IP configuration is not set from the Network Configurator, the EtherNet/IP Unit will operate with the following default values.

Setting	Operating status
IP address	192.168.250.Node_address
Subnet mask	255.255.255.0 (class C mask)
Default gateway	None (IP routing disabled)
Preferred DNS server	None
Alternate DNS server	None
Host name	None
Domain name	None
Baud rate	Auto-detect

IP Address

Set the EtherNet/IP Unit's local IP address. The default IP address is determined by the following formula.

Default IP address = 192.168.250.IP address setting switch value

The IP address setting switch value is set with the EtherNet/IP Unit front rotary switches. Refer to *3-7-3 Switches* for how to set the IP address using the rotary switch.

When the NE2A-ENS21 EtherNet/IP Unit is mounted to an NE2A-series CPU Unit and the IP address is not set from the Network Configurator, the EtherNet/IP Unit will operate with the default IP address.

Subnet Mask

All bits corresponding to the bits in the IP address used as either the network number or the subnet number are set to 1, and the bits corresponding to the host number are turned OFF.

If no subnet mask is set or if an illegal value is set, the following values will be used depending on the IP address class.

Class	Subnet mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

With the default setting (0.0.0.0), a subnet mask corresponding to the IP address class is used.

Default Gateway

Sets the default gateway's IP address. This setting is not required when the default gateway is not being used.

Preferred DNS Server and Alternate DNS Server

At this time, the EtherNet/IP Unit is not equipped with any functions that require a DNS server, so these settings are not used.

Domain Name

The EtherNet/IP Unit does not use domain names in actual communications.

Baud Rate

Set the communications baud rate.

Setting	Meaning
Auto (See note.)	The baud rate of the switching hub is detected automatically. If possible, the Unit operates in 100Base-T (full duplex).
10MBps Half Duplex	Operates in 10Base-T, half duplex.
10MBps Full Duplex	Operates in 10Base-T, full duplex.
100MBps Half Duplex	Operates in 100Base-TX, half duplex.
100MBps Full Duplex	Operates in 100Base-TX, full duplex.

Note This is the default setting.

Note Set the EtherNet/IP Unit's link settings to the same communications settings as the connected switching hub. If the settings are not the same, the link will become unstable and prevent normal communications. The following table shows the allowed settings for each switching hub communications mode.

EtherNet/IP Unit settings / Switching Hub settings		Auto-negotiation	10 Mbps (fixed)		100 Mbps (fixed)	
			Full duplex	Half duplex	Full duplex	Half duplex
Auto-Negotiation		Best	-	OK	-	OK
10 Mbps (fixed)	Full duplex	-	OK	-	-	-
	Half duplex	OK	-	OK	-	-
100 Mbps (fixed)	Full duplex	-	-	-	Best	-
	Half duplex	OK	-	-	-	OK

5-3 DeviceNet and EtherNet/IP Routing

5-3-1 Routing between DeviceNet and EtherNet/IP Networks

Safety Communications and Standard Communications cannot be used to route data transmissions between NE2A-series DeviceNet Safety Units and EtherNet/IP Safety Units.

To transfer data between a DeviceNet Safety Unit and an EtherNet/IP Safety Unit with Safety Communications, additional programming is required, for example, to apply the values of input variables to output variables.

Data can be transferred with Standard Communications by allocating DeviceNet Master input data (data for monitoring) to EtherNet/IP tag link data, eliminating the need to create a program to copy the data.

Note Explicit message communications can be used to route transmissions between Communications Units.

5-3-2 Routing with an Ethernet Switching Hub

This section explains EtherNet/IP communications routing with an OMRON W4S1-series Ethernet Switching Hub.

Same Network Addresses

Safety Communications can be used when the connection type is set to either Single Cast or Multicast.

Standard Communications can be used when the connection type is set to either Point to Point or Multicast. However, you cannot specify the delay for calculating the response time when the connection type is set to Multicast.

Different Network Addresses

Routing Safety Communications is possible when the connection type is set to Single Cast, but not possible when it is set to Multicast. (A timeout error will occur.)

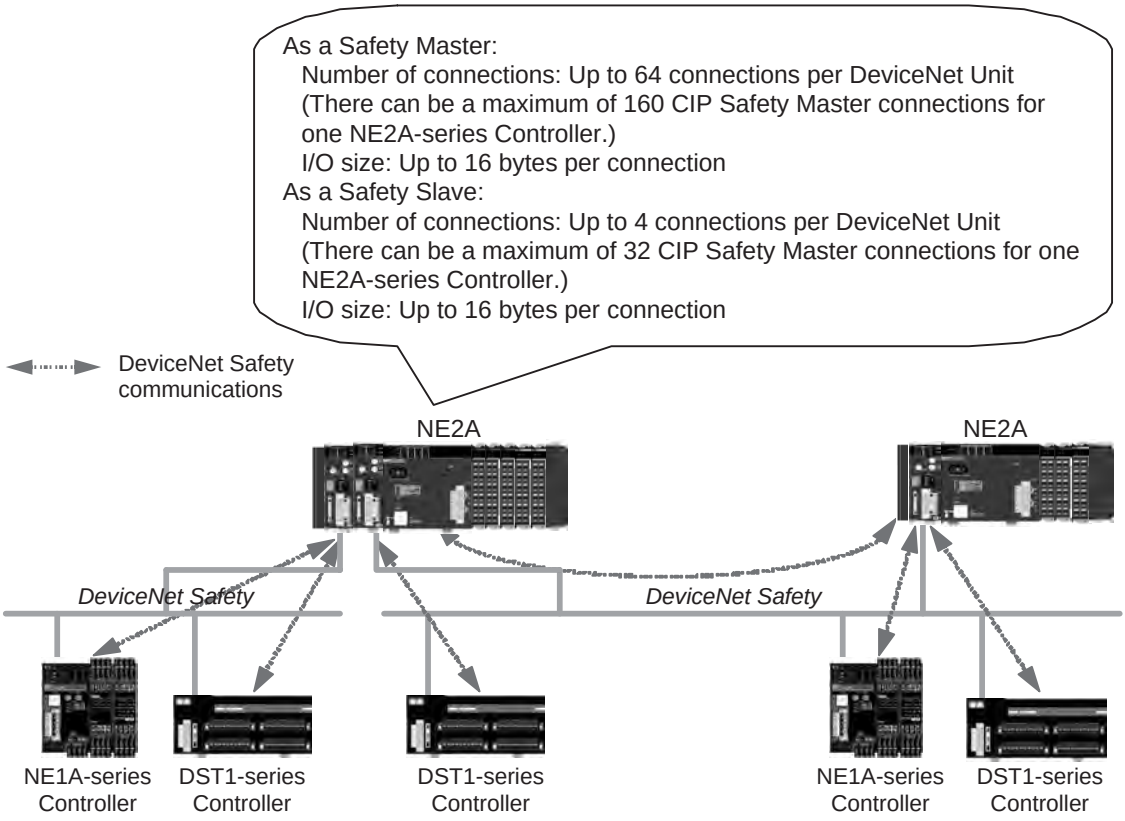
Routing Standard Communications is possible when the connection type is set to Point to Point, but not possible when it is set to Multicast. (A timeout error will occur.)

5-4 DeviceNet Safety Communications

5-4-1 Outline of DeviceNet Safety Communications

A remote Safety I/O system can be constructed using DeviceNet Safety. Up to six DeviceNet Safety Units can be connected in one NE2A-series Controller. Slaves can be distributed using more than one DeviceNet Safety Unit when the safety control area expands. This reduces the area of usage per network and improves response performance.

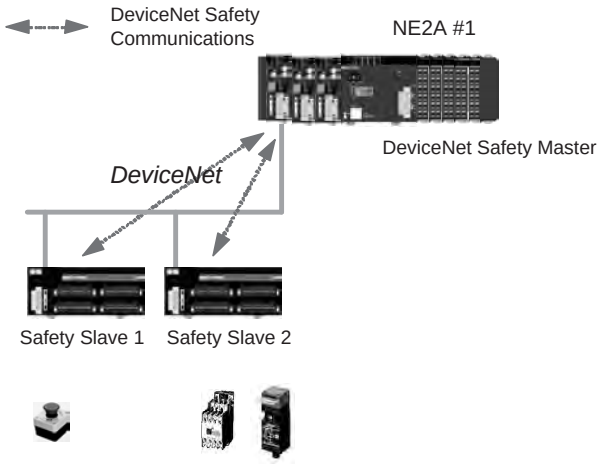
The mounted Units can be flexibly used as Safety Masters, Safety Slaves, Standard Masters, and Standard Slaves.



Note DeviceNet Safety Communications are not possible with an NE1A-series Safety Master and NE2A-series Safety Slaves.

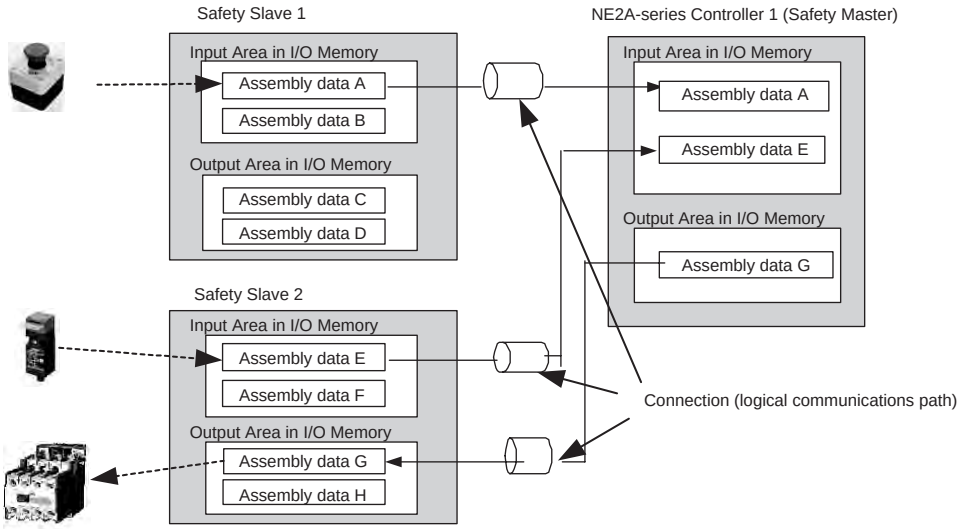
5-4-2 Setting Safety Connections

Set the Safety Connections to perform Safety I/O Communications between the Safety Master and Safety Slaves. A connection is a logical communication path between a Master and a Slave.



Set the connection between NE2A-series Controller 1 and Slave 1 to allocate the Slave 1 emergency stop switch to the NE2A-series Controller 1 input.

Once the connection is set, the ON/OFF status of the emergency stop switch will be periodically sent to NE2A-series Controller 1.



Two connections are used for the Safety Connection between the NE2A-series Controller 1 Safety Master and Safety Slave 2 for the input assembly data and output assembly data. Assembly data is a collection of input data or output data used for communications between a Master and Slave. (Refer to *5-8 Remote I/O Allocations*.)

The I/O assemblies set in this way are displayed in the I/O tag lists as I/O tags for the Slaves in the Logic Editor. The I/O tags can be used to program the NE2A-series Controller without considering specific memory addresses.



Setting the Connection Information for the Safety Master

The parameters that are set are listed in the following table.

Parameter	Description	
I/O connection	Specify the data that you want to allocate to the Safety Master from the I/O data set in *5-8 Remote I/O Allocations*.	
Open type	Configure the Safety Slave	The Safety Slave is configured when the connection is established.
	Check the safety signature	The safety signature is checked in the Safety Slave when a connection is established to make sure that the configuration is correct. This is normally set when establishing a connection between a Safety Network Controller and DST1-series Safety I/O Terminals.
	Open only	The Safety Slave establishes the connection without checking the safety signature. This is normally set when establishing a connection between Safety Network Controllers.
Connection type	Multicast connection	This connection type can be selected only for a Safety Input Slave. When a multicast connection is selected, a Safety Input Slave can transmit input data to a maximum of 15 Safety Masters by using a multicast connection. These Safety Masters are classified as the same multicast group if the I/O data and EPI values specified in I/O connection are the same. This connection type can be selected even for one Safety Master.
	Single Cast connection	The Safety Master and Safety Slave establish a 1:1 connection and perform Safety I/O Communications.
Expected Packet Interval (EPI)	The EPI sets the interval at which the Safety Master and Safety Slave communicate safety data. Devices that send data to the network send data at the set time interval and monitor whether the devices set to receive the data can receive the correct data at the specified interval. If it cannot, the connection is disengaged and the safe state is entered. The EPI value affects the safety response performance. Refer to *8-2 Calculating Safety Response Performance*.	

Parameter	Description	
Advanced connection settings	Time out multiplier	This parameter is used to set the number of timeouts used to determine if an error has occurred in communications. If the parameter value is high there will be less communication errors but it will take longer to reach an error and affect the response performance. The default is two timeouts (i.e., only one timeout is allowed).
	Network delay multiplier	This parameter is used when calculating the reaction time as a percentage of the EPI. The default is 100%.
	ID allocation	This parameter is used to allocate an ID to the Safety Connection. There is a limit to the ID numbers that can be allocated by the Master and Slave. If the limit is exceeded for one, ID numbers for the other can be used. The Master allocates produced connection IDs. The Safety Slave checks the produced IDs. NE2A-series Controllers do not use this parameter.

⚠ WARNING

Serious injury may possibly occur due to loss of required safety function. Make sure that the Safety Master and Slave have the correct configuration when setting an open type to “open only.”



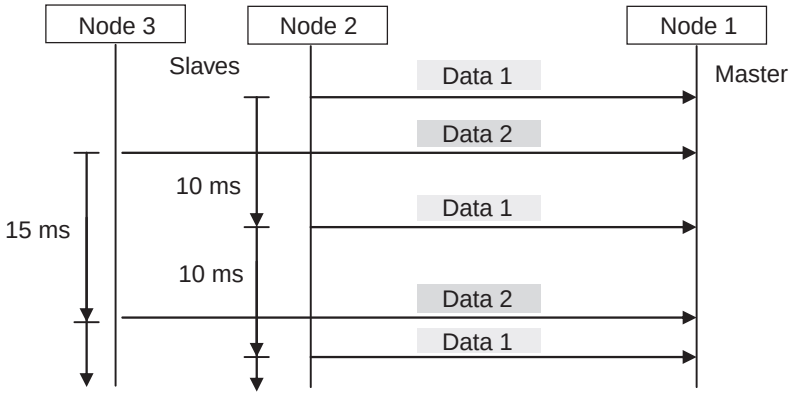
Expected Packet Interval (EPI)

The EPI is the communications interval for Safety Data between a Safety Controller and the Safety Slaves. A device transmits data to the network during the set interval and the receiving device monitors to see if the data is received normally within the data transmission interval. If the data is not received normally, the connection is broken and the devices go to the safe state.

The EPI values affect the safety response performance (reaction time).

Example: One connection each is set between node 1 (the Master) and nodes 2 and 3 (Slaves).
The EPI for the connection with node 2 (data 1) is set to 10 ms.
The EPI for the connection with node 3 (data 2) is set to 15 ms.

In this example, data 1 is transmitted from node 2 to node 1 every 10 ms and data 2 is transmitted from node 3 to node 1 every 15 ms.



An EPI is set for each connection.

The minimum EPI that can be set for an NE2A-series Controller is the larger of the following two values.

a. The NE2A peripheral servicing cycle time

b. The time required for Safety I/O Communications

c. The cycle time of the Safety Slave being communicated with
If the communications partner is a DST1-series Slave, the cycle time is 6 ms.

If the communications partner is an NE2A-series Slave, check its peripheral servicing cycle time.

d. The time required for Safety I/O Communications with the NE2A-series Slave that is being communicated with*3

If the communications partner is an NE2A-series Slave, check its EPI required for Safety I/O Communications.

Note (1) Set the EPI for each Safety Connection to a time longer than the peripheral servicing cycle time of the Safety Network Controller.

(2) If the communications partner is a NE2A-series, NE1A-series, or NE0A-series Slave, its cycle time is not checked. Use the Network Configurator to confirm that the set EPI is longer than the cycle time of the NE2A-series, NE1A-series, or NE0A-series Slave.

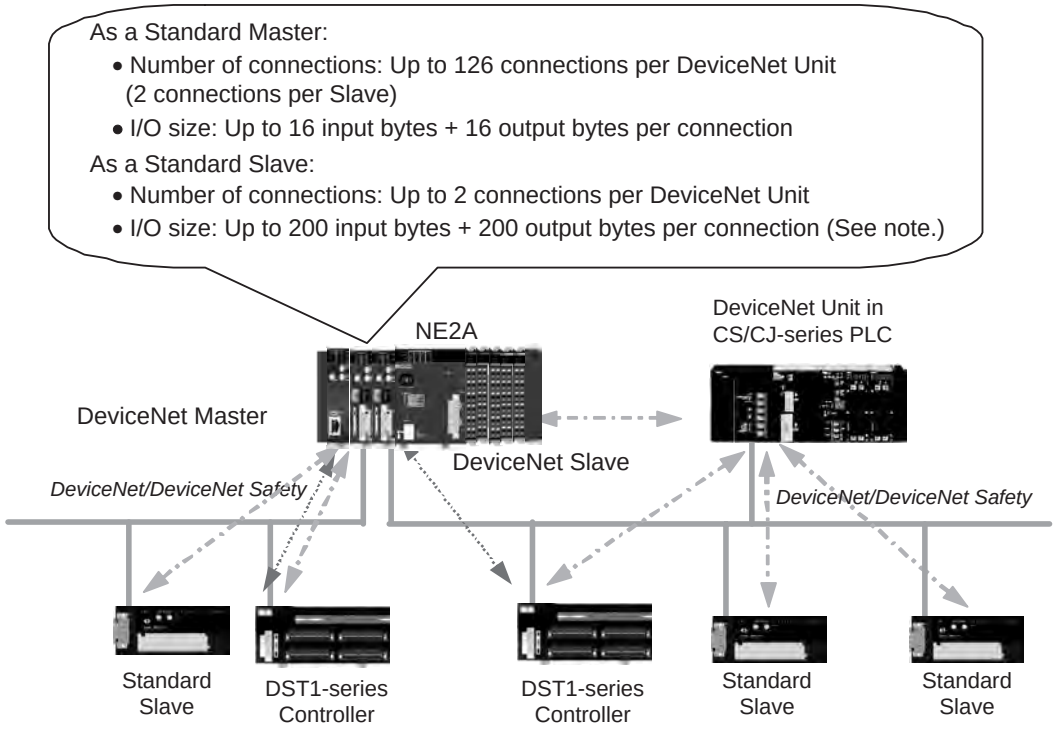
5-5 DeviceNet Standard Communications

5-5-1 Outline of DeviceNet Standard Communications

Monitoring systems using Standard PLCs can be constructed using DeviceNet Standard Communications. A Standard Master is used to input/output Standard signals used for safety control. A Standard Slave is used for transmission of monitor data and interlock signals between Controllers with DeviceNet Master Units connected to them. Data can be exchanged between the Standard Master and Standard Slave without user programming using Standard I/O Communications.

DeviceNet Safety Communications

DeviceNet Standard Communications



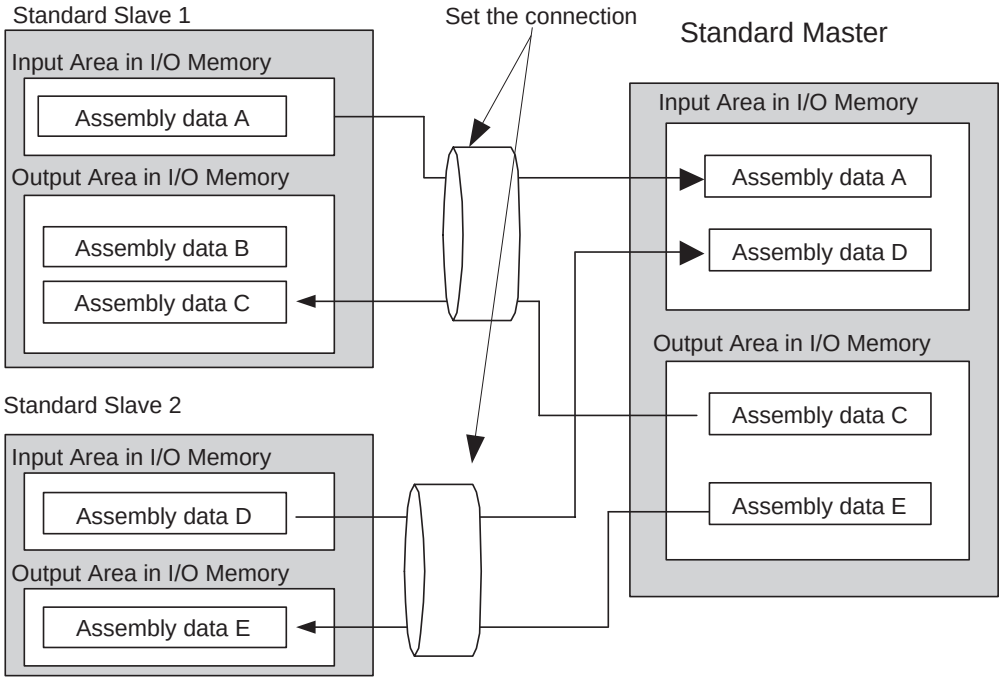
Note The I/O size of the connected Safety Master cannot be exceeded.

⚠ WARNING

Serious injury may occasionally occur due to loss of required safety functions. Do not use Standard I/O Communications data to configure a safety system. Standard I/O Communications data is non-safety data. The measures necessary for safety data are not taken during data communications.

5-5-2 Standard Connection Settings

Set Standard Connections to perform Standard I/O Communications between the Standard Master and Standard Slaves.



A Standard Connection sends and receives input and output assembly data using one connection. This input and output assembly data is displayed on the I/O tag list as I/O tags (Standard Input or Standard Output) for each Logic Editor Slave. By using these I/O tags, you can create programs without being aware of the memory addresses of the NE2A-series Controllers.

Setting the Connection Information for the Standard Master

The parameters that are set are listed in the following table.

Parameter	Description	
Connection pass	Specify data that you want to allocate to the Standard Master from the I/O data set in *5-8 Remote I/O Allocations*.	
I/O type *1	Poll	The Master device sends output data to each Slave device and these act as triggers for the Slave devices to send input data to the Master device. This I/O type is mainly used when the Slave device is an actuator and there is a large amount of data to be exchanged.
	Bit strobe	The Master device simultaneously broadcasts a trigger signal to all Slave devices and the Slave devices send input data to the Master device. This I/O type is suited for collecting small amounts of data when the Slaves are devices such as sensors. Inputs to the Master can be up to 8 bytes. (Output data cannot be sent from the Master.)
	COS (Change of State)	The Master or Slave sends output data or input data at one of the following times. • Constant period (Heartbeat timer *2) • When a software switch in the Master or Slave program changes state The load on the communications network can be reduced because data can be sent only when it is necessary. COS is the preferred connection over a Poll or Bit Strobe connection. The communications cycle may become longer if the COS transmission frequency is high or there is a large amount of data. COS is used when data changes less frequently (approx. 100 ms min.) and there is only a small amount of data, but the data has a high priority.
	Cyclic	Slave devices send data at a constant interval regardless of send requests from the Master device. If the Slave device is a temperature controller, it is suitable for collecting data at a constant interval. The Master or Slave sends output data or input data at a constant time interval (Heartbeat Timer *2). Cyclic is the preferred connection for a Poll or Bit Strobe connection. The communications cycle may become longer if there is a large amount of data for a Cyclic Connection. It is suitable when the data changes less frequently and the amount of data is small.
Communications cycle Time	The communications cycle time is the time taken to process the I/O data communications for a Slave after the I/O data communications has been processed for the same Slave. The communications cycle time is also used to calculate the maximum I/O response time. The communications cycle time depends on various factors, such as whether there is only one Master or there are multiple Units in the network or whether a message communication was performed or not.	

*1 I/O Type Restrictions

- Connections can be specified for each Slave
- COS and Cyclic connections cannot be used simultaneously together.
- When Poll/COS or Poll/Cyclic connections are both selected for a single output Target, the maximum output data size is 16 bytes per connection. Up to 32 input bytes can be set for two connections.

*2 The larger of the following two values is used as the interval for the heartbeat timer. However, the minimum is 20 ms and the timer accuracy is 10 ms.

- Heartbeat timer set value (ms)
- Twice the communications cycle timer (ms)

Communications Cycle Time

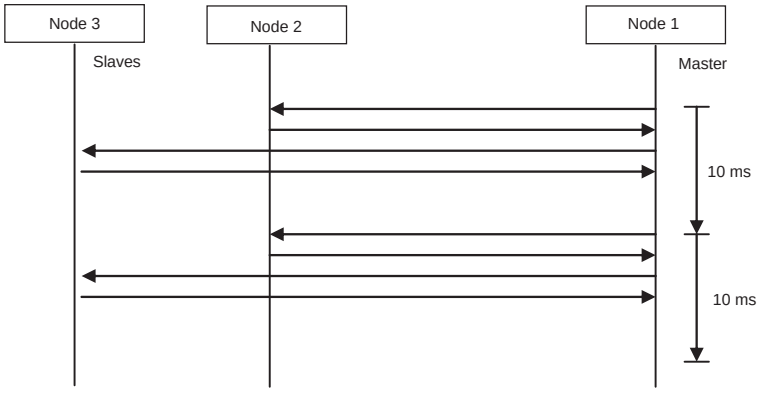
The communications cycle time is the time required from processing I/O data communications to the Slaves until processing I/O data communications to the Slaves again. The communications cycle time is also used to calculate the maximum I/O response time.

The communications cycle time depends on many factors, such as the number of Masters on the network and whether message communications are being performed.

Example for Poll I/O Connection

One connection each is set between node 1 (the Master) and nodes 2 and 3 (Slaves).

Node 1 performs communications with node 2 and then node 3 on a 10-ms communications cycle time.



The communications cycle time is set in the Master. The Master and the Slaves to which the connections are set perform data communications using the same communications cycle time.

Device Information

A Standard Master can prevent malfunction by comparing the following parameters with the Slaves that are actually connected online.

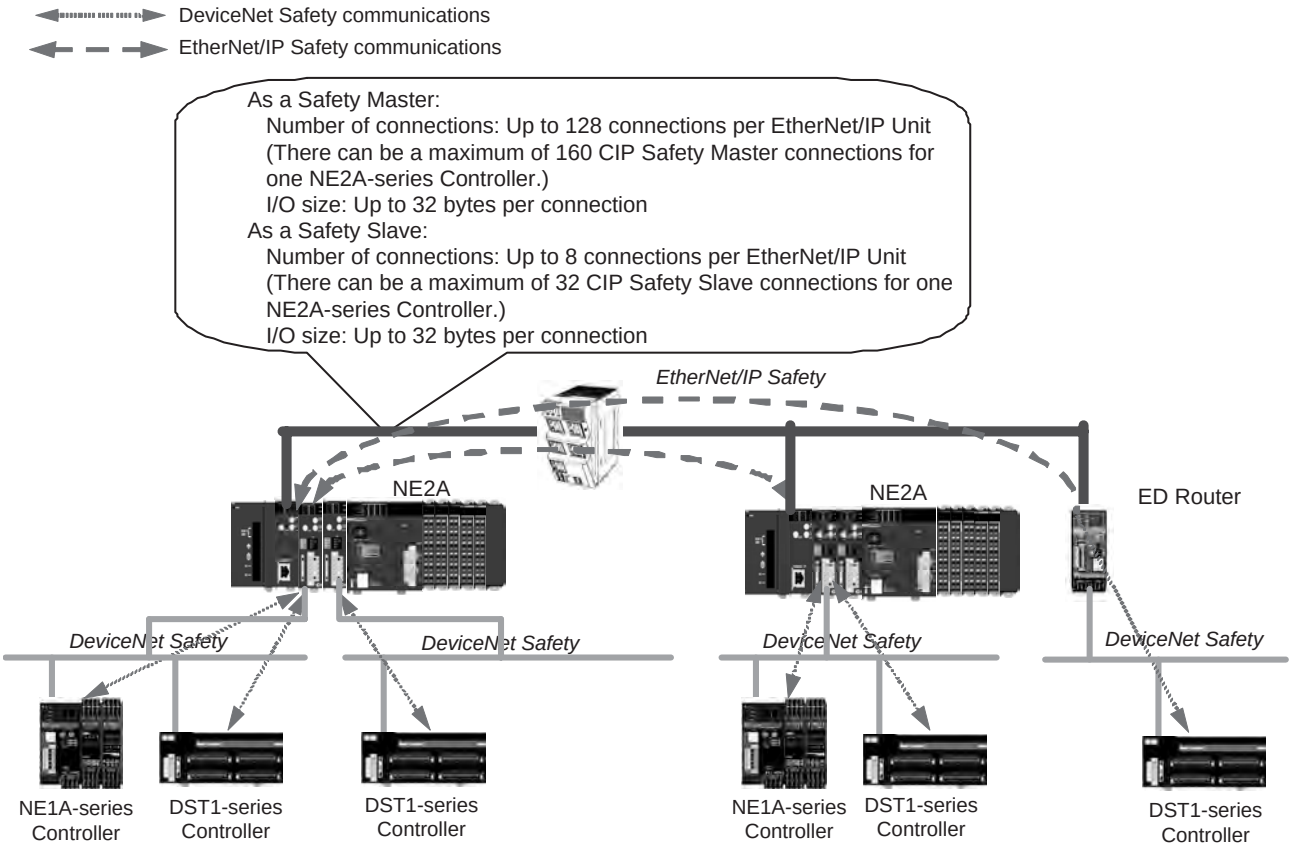
Parameter	Description
Vendor	Value unique to the manufacturer.
Device type	Value unique to the product type.
Product code	Value unique to the product model.

5-6 EtherNet/IP Safety Communications

5-6-1 Outline of EtherNet/IP Safety Communications

EtherNet/IP Safety performs safety communications on the Ethernet, which also functions as a generic network. Data can be exchanged between the Safety Master and Safety Slaves without user programming using Safety I/O Communications for EtherNet/IP Safety.

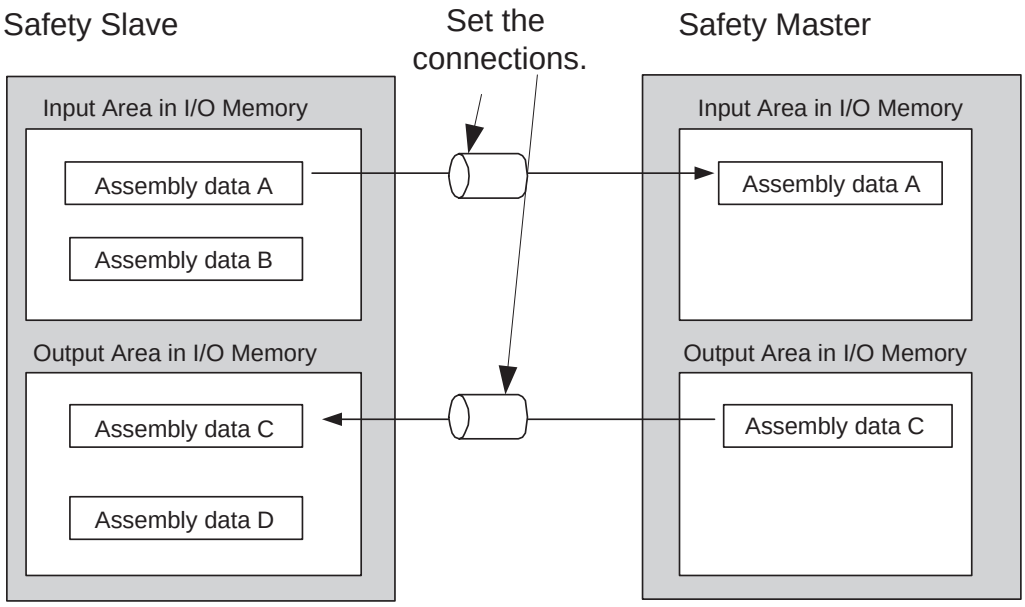
One NE2A-series Controller can simultaneously function as a Safety Master and Safety Slave, and can be a Target for Standard Communications with EtherNet/IP communications.



IMPORTANT The NE2A-series Controllers must not be connected to open transmission systems.

5-6-2 Setting the Safety Connections

Set the Safety Connections to perform Safety I/O Communications between the Safety Master and Safety Slaves. Set the connections for EtherNet/IP Safety Communications in the same way as for DeviceNet Safety Communications.



Setting the Connection Information for the Safety Master

Refer to *5-4-2 Setting Safety Connections* for information on the settings.

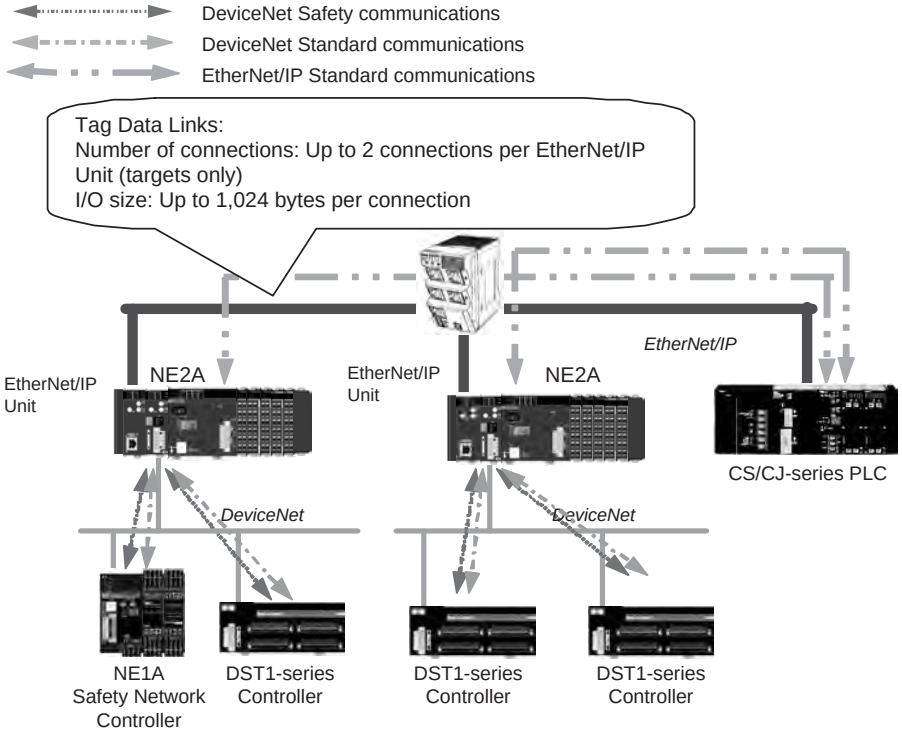
5-7 EtherNet/IP Standard Communications

5-7-1 Outline of EtherNet/IP Tag Data Link Communications

Tag Data Link communications (Targets only) can be used by mounting an EtherNet/IP Unit on a NE2A-series Controller. Data can be shared between devices (i.e., Controllers) that support Tag Data Links.

EtherNet/IP Tag Data Links can be used mainly in the following applications.

- Data communications between Controllers that support EtherNet/IP Tag Data Links and NE2A-series Controllers.
- Data communications between Controllers that support EtherNet/IP Tag Data Links and Safety Devices on a DeviceNet network via NE2A-series Controllers. (DeviceNet Safety Communications or DeviceNet Standard Communications are used between the NE2A-series Controller and the Safety Device.)



⚠ WARNING

EtherNet/IP tag link communications data is non-safety data. The measures necessary for safety data are not taken for this data during generation. Therefore, do not use this data to configure a Safety Control System.

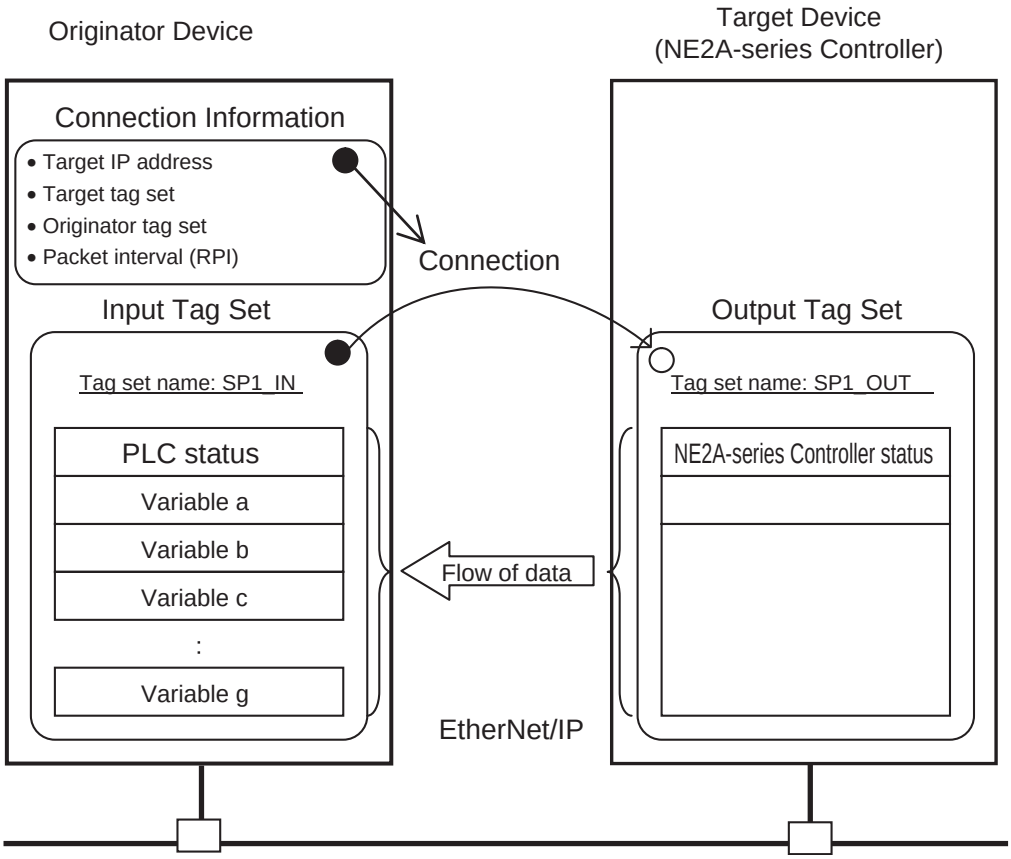
IMPORTANT The NE2A-series Controllers must not be connected to open transmission systems.

Note The NE2A-series Controller can function only as a Target. It cannot function as an Originator. To set the Originator, refer to the user's manual for the EtherNet/IP Unit that will be the Originator, such as a Standard PLC.

5-7-2 Setting Tag Data Link Connections

Tag Data Link communications functions by joining tag sets with connections.

In the following example, Originator variables a, b, c, ..., g (inputs) are made into a tag set named SP1_IN, and the Target variables i and ii (outputs) are made into a tag set named SP1_OUT for the connection.



A tag set contains either input (consume) or output (produce) data. Therefore, one tag set cannot contain both input and output variables. Furthermore, one input variable cannot be registered in more than one input tag set.

One tag set can be assigned to one connection with the EtherNet/IP Unit. Variables are set for tag sets using the Network Configurator.

Connection Information Set for Tag Data Links

The following parameters are set for Tag Data Links.

Parameter	Description
Connection name	Sets the name for the connection. Any name can be used.
Connection I/O type	When using NE2A-series Controllers, select from Input Only, Output Only, or Input & Output.
Target variable	Set the Target node's tag set. • IN: Set the output (produce) tag set. • OUT: Set the input (consume) tag set.
Originator variable	Set the Originator node's tag set. • IN: Set the output (produce) tag set. • OUT: Set the input (consume) tag set.

Parameter	Description
Connection type	Set whether the data is sent using a multicast or unicast connection. • Multicast Connection: Set a multicast connection when the same data is shared by multiple nodes (four nodes max.). This setting is usually used. • Point-to-Point Connection Set a point-to-point connection when the same data is not being shared by multiple nodes. In a unicast transmission, other nodes are not burdened with an unnecessary load.
Packet interval (RPI)	Set the packet interval (RPI) of each connection between the Originator and Target. The interval can be set between 1 and 10,000 ms, in 1-ms units. The default setting is 50 ms (data refreshed once every 50 ms).
Timeout value	Set the time until a connection timeout is detected. The timeout value is set as a multiple of the packet interval (RPI) and can be set to 4, 8, 16, 32, 64, 128, 256, or 512. The default setting is 4 times the packet interval (RPI).

⚠ WARNING

Serious injury may possibly occur due to loss of required safety function. Do not use Standard I/O Communications data to configure a safety system. Standard I/O Communications data is non-safety data. The measures necessary for safety data are not taken during data communications.



Multicast and Point-to-point Connections

The connection type for Tag Data Link connections can be set to a multicast connection or a point-to-point connection.

With a multicast connection, one tag set can be sent to multiple Consumers using one packet. (There is a maximum of four Originators.)

With a point-to-point connection, a tag set must be sent separately to each Consumer, so the same number of packets is required as the number of Consumers.

Thus, using a multicast connection will reduce the communications traffic when sending the same tag set to more than one Consumer. To use multicast connections, however, a switching hub with a multicast filter is required except when sending the tag to all nodes. If a switching hub without a multicast filter is used, the multicast packet is broadcast to the entire network, so unnecessary packets are sent to some nodes, which can increase communications traffic.

To use a multicast connection to send a tag set to multiple Consumers with one packet, the tag set, connection type, RPI, timeout value, and connection type (i.e., multicast) must be the same for all nodes.

Setting and Checking the Multicast Group Configuration

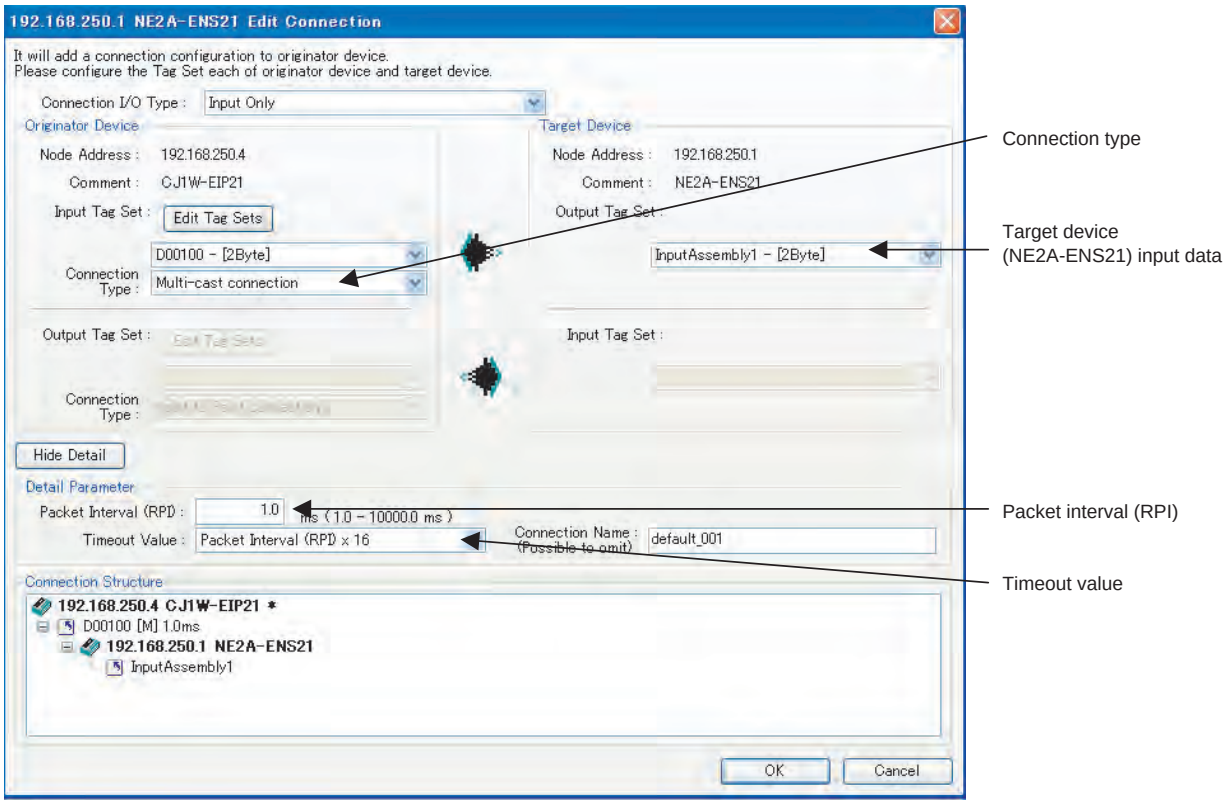
If you use the Network Configurator, set the following values for all nodes to configure a multicast group.

Settings:

- Connection type: Multicast connection
- Target device (NE2A-ENS21) input data: Set the same input tag set.
- Packet interval (RPI): Set the same value.
- Timeout value: Set the same value.

1. When Less Than Five Originators Perform Multicast Communications

Make the settings on the Edit Connection Dialog Box for the originator device on the Network Configurator. (Click the **Show Detail** Button in the Edit Connection Dialog Box to set the advanced parameters.)

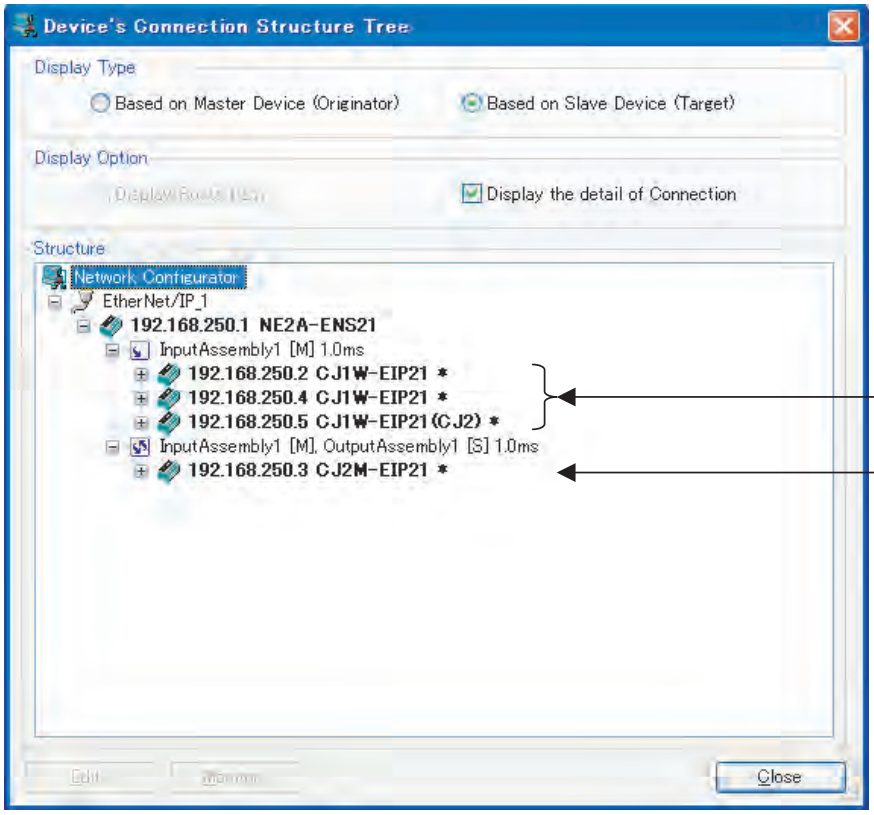


The multicast group is configured by setting the connection type, target device (NE2A-ENS21) input data, packet interval (RPI), and timeout value to the same values in the originator settings.

Use the following procedure to check the configuration of the multicast group.

Right-click on the EtherNet/IP Network Window and select ***View Device's Connection Structure Tree***.

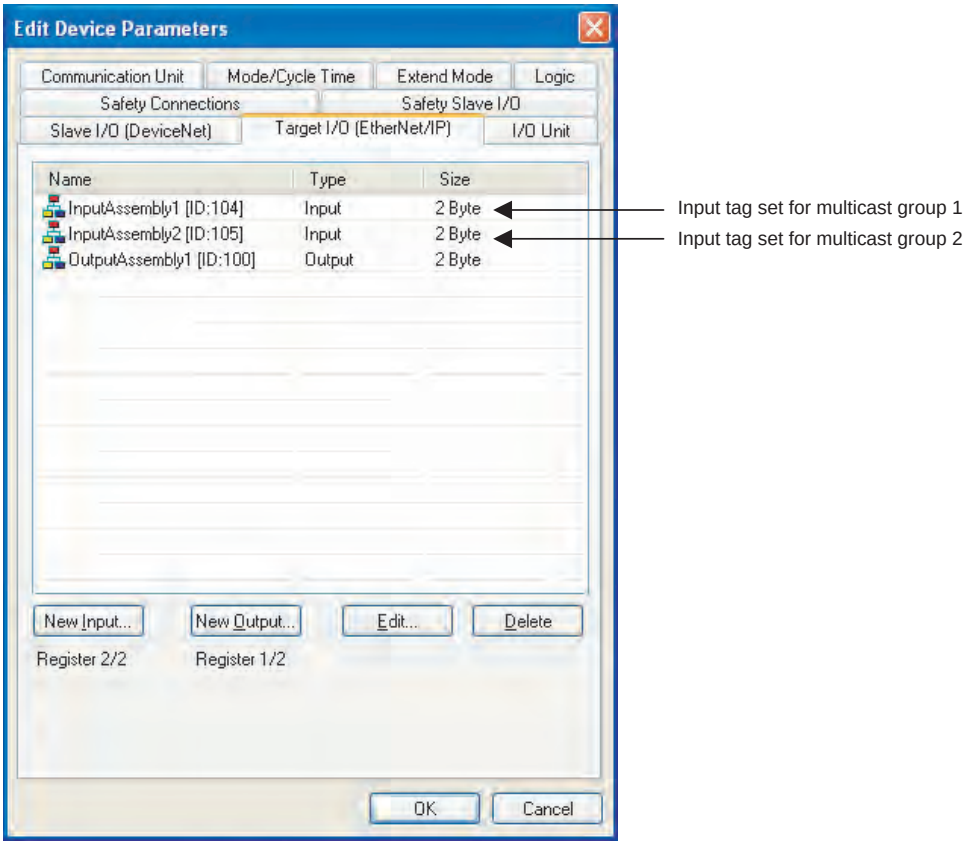
In the Device's Connection Structure Tree Dialog Box, select the *Based on Slave Device (Target)* Option in the Display Type Area. The communications settings for the target devices will be displayed. If the settings that are required to configure a multicast group are all the same, a multicast group will be displayed as shown below.



Note If the input data in the originator settings are the same as the rest of the multicast group, but the output data is different for a node, the node will be displayed as a different group in the dialog box. However, this node is considered to be in the same multicast group for the input data. If the output data is set at the same time, make sure the inputs settings are the same on the Edit Connection Dialog Box for the originator.

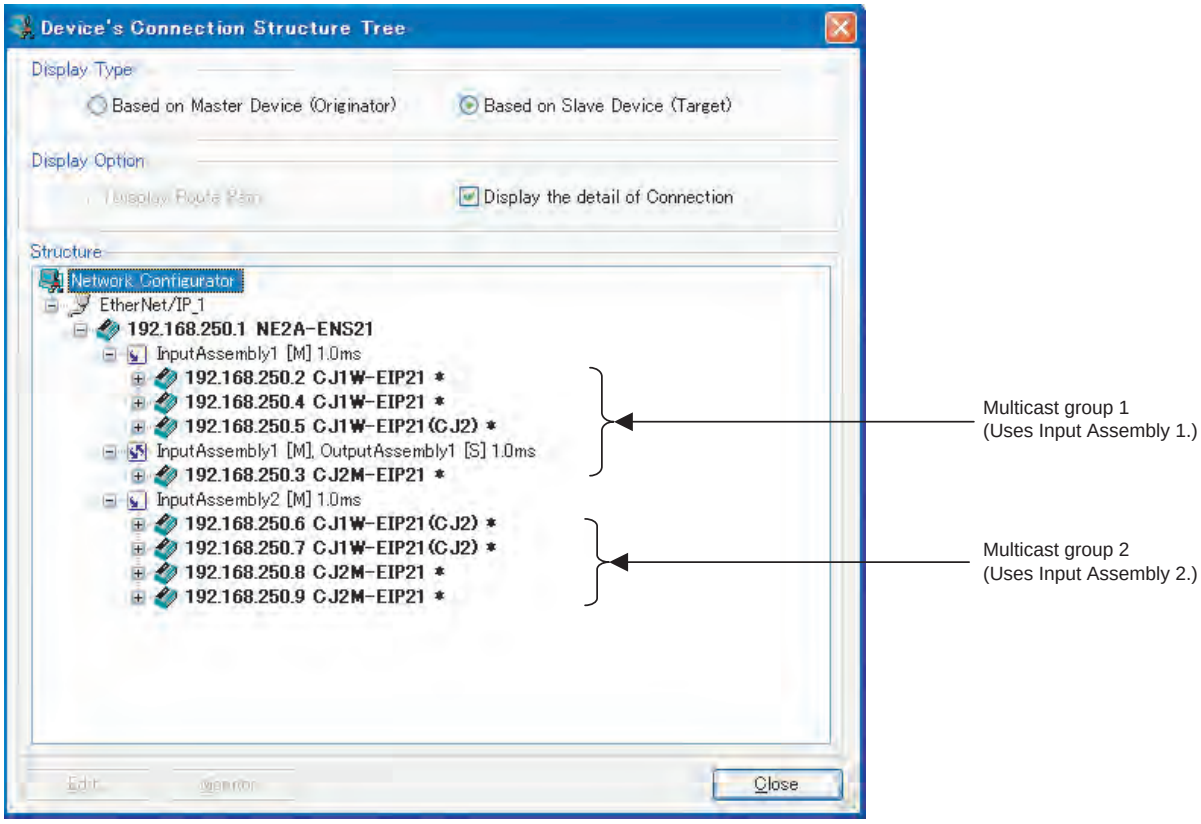
2. When More Than Four or Less Than Nine Originators Perform Multicast Communications

If multicast communications are necessary for more than the maximum number of originators (4) that can communicate in one multicast connection, you can configure two multicast groups for the NE2A-ENS21.
First, set the input tag set for each multicast group in the Target I/O (EtherNet/IP) settings of the NE2A-SCPU01.



Then, use the procedure given above in *When Less Than Five Originators Perform Multicast Communications* to set each of the multicast groups in the settings on the Edit Connection Dialog Box for the originator. (Set the same connection type, target device (NE2A-ENS21) input data, packet interval (RPI), and timeout value for each of the multicast groups in the originator settings.)

After you finish the settings, right-click on the EtherNet/IP Network Window and select ***View Device's Connection Structure Tree***. In the Device's Connection Structure Tree Dialog Box, select the *Based on Slave Device (Target)* Option in the Display Type Area. The communications settings for the target devices will be displayed.
If there are eight originators in two multicast groups, the Structure Dialog Box will appear as shown below.



In this example, two multicast groups are configured for the NE2A-ENS21. (The originator with IP address 192.168.250.3 is also set for communications with Output Assembly 1 does not appear to be part of the group on the display, but the same communications settings as for Input Assembly 1 are used, so it is part of multicast group 1.)

Note For the NE2A-ENS21, each multicast group can contain a maximum of four originators. You cannot set more than four originators in one multicast group.

Requested Packet Interval (RPI)

The RPI is the interval for data communications between an Originator and a Target. A device that transmits data on the network sends the data at the set time interval.

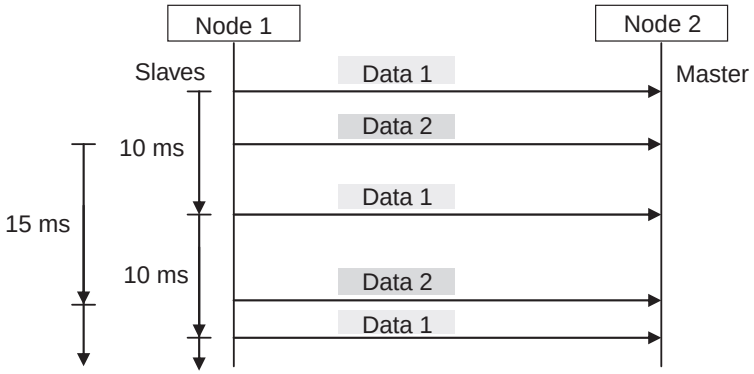
Example:

Two Tag Data Link connections are set between node 2 (the Originator) and node 1 (the Target).

The RPI for connection 1 (send data 1) is set to 10 ms.

The RPI for connection 2 (send data 2) is set to 15 ms.

In this example, data 1 is transmitted from node 1 to node 2 every 10 ms and data 2 is transmitted from node 1 to node 2 every 15 ms.



An RPI is set for each connection.

5-8 Remote I/O Allocations

5-8-1 Outline of Remote I/O Allocations

A NE2A-series Controller defines assembly data for communications as a DeviceNet Safety Slave, EtherNet/IP Safety Slave, DeviceNet Standard Salve, and EtherNet/IP Tag Data Link Target. (Tag sets are also defined in the same way as assembly data.)

Assembly data is a collection of input data or output data used to communicate between a Master and Slave or an Originator and Target of each type of communications. By predefining the data, it can be transmitted without relying on user programming. Variables, local I/O information, remote I/O information, and status information can be freely combined and allocated to the assembly data.

Types of Assembly Data That Can Be Set

Data that is input to the Master is called an input assembly and data that is output from the Master is called an output assembly.

The following types of assemblies can be created for a NE2A-series Controller. The following table gives the maximum number of assemblies that can be created and the maximum number of data items that can be allocated for each assembly type.

Type	Number of assemblies that can be created	Maximum number of data items that can be allocated
Safety Target I/O: Input assembly	8	64
Safety Target I/O: Output assembly	8	64
Slave I/O (DeviceNet): Input assembly	8	64
Slave I/O (DeviceNet): Output assembly	8	64
Target I/O (EtherNet/IP): Input assembly	2	512
Target I/O (EtherNet/IP): Output assembly	2	256

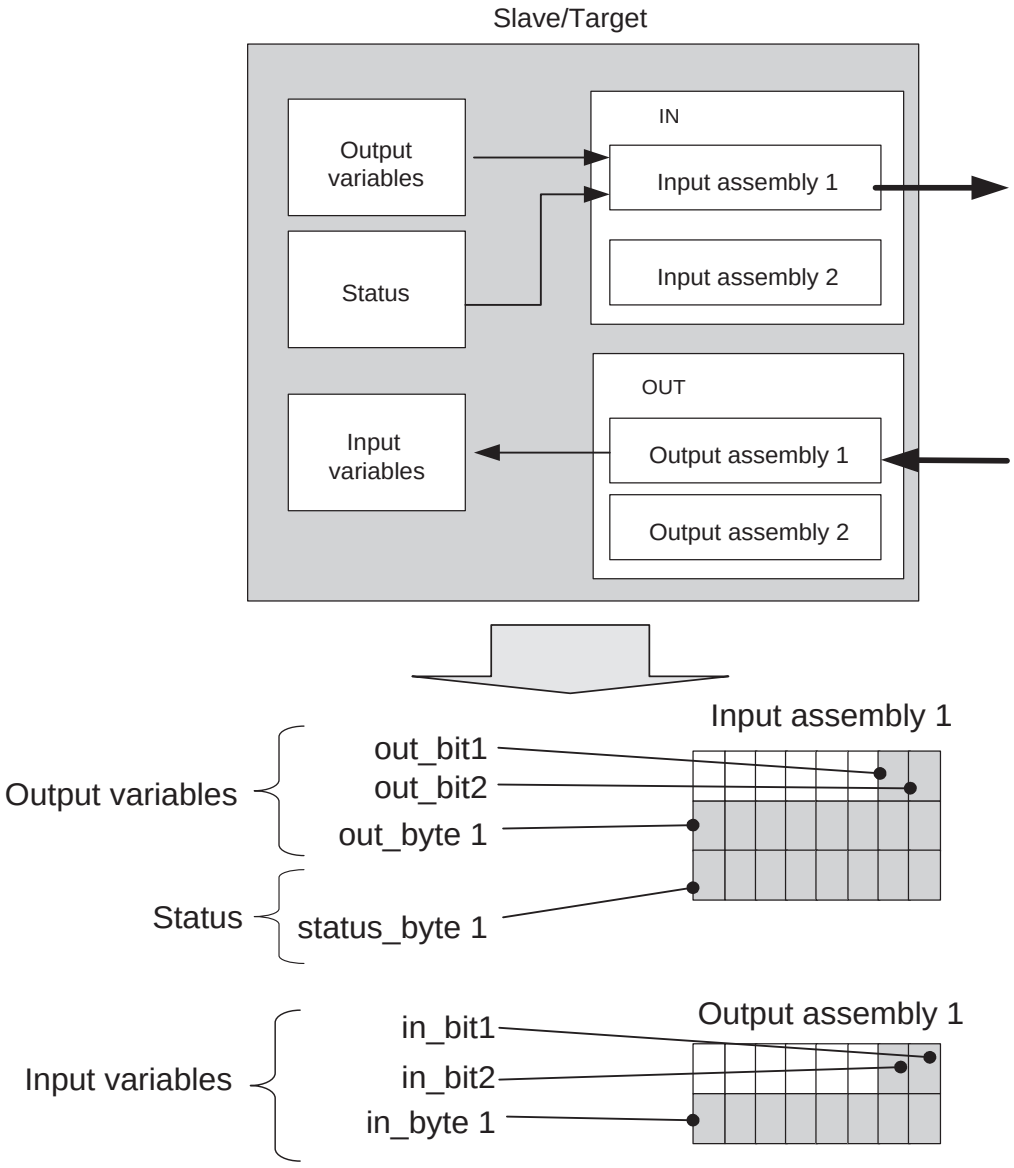
An input assembly (produce) can be used in more than one connection. An output assembly (consume) can be used in only one connection.

Note The Network Configurator can export data names and data types allocated within the assemblies in a form that can be imported to PLC Support Software, such as the CX-Programmer.

Creating Assemblies

The **assembly** format created in the Slaves can be used in the Master for connections for DeviceNet Safety Communications, DeviceNet Standard Communications, and EtherNet/IP Safety Communications.

For EtherNet/IP Tag Data Links, tag sets must be created in both the Originator and Target. (Refer to *5-7-2 Setting Tag Data Link Connections*) The data that can be set for assemblies and tag sets are described on the following pages.



Note BOOL data can be arranged in BYTE, WORD, or DWORD data. If longer variables, such as BYTE variables, are placed between continuous BOOL variables, the total data size will change.

5-8-2 Configuring Assemblies

Safety Communications

Data That Can Be Set in an Input Assembly

Category	Type	Allocatable units
Variables	Output variables	BOOL, BYTE, WORD, or DWORD

Data That Can Be Set in an Output Assembly

Category	Type	Allocatable units
Variables	Input variables	BOOL, BYTE, WORD, or DWORD

Standard Communications

Refer to *5-8-3 Data Elements Set in Assemblies* for information on the data elements. (The Reference column in the following table gives the section in *5-8-3*.)

Data That Can Set in an Input Assembly

Category	Type				Reference	Allocatable units
Variables	Output variable				---	BOOL, BYTE, WORD, or DWORD
Status	General status				1)	• All • BOOL (bit)
	Error status				2)	
	Safety Connection normal status				3)	
	Safety Connection error status				4)	
	Fault present				5)	• All
Remote Standard I/O	DeviceNet Unit	Status	Unit status 1/2		7)	• All • Communications Unit • BOOL (bit)
			Master status		8)	
			Slave status		9)	
			Registered Slave table		10)	
			Normal Slave table		11)	
		Master I/O data	Node	Input data	12)	• Communications Unit
	EtherNet/IP Unit		Unit status 1/2		14)	• All • Communications Unit • BOOL (bit)
			Communications status 1/2/3		15)	
Local I/O	Output Unit		Output data		16)	• All • BOOL (terminal)
			Local I/O status		18)	
			I/O Unit error status		19)	
			Local I/O cause of the error		20)	
	Input Unit		Input data		17)	
			Local I/O status		18)	
			I/O Unit error status		19)	
			Local I/O cause of the error		20)	
Remote Safety I/O	Network	Slave	Output data		21)	• Input data or output data • BOOL (bit)
			Input data		22)	

Data That Can Be Set in an Output Assembly

Category	Type				Reference	Allocatable units
Variables	Input variable				---	BOOL, BYTE, WORD, or DWORD
Status	Safety Connection communications reopen switch				6)	• All • BOOL (connection)
Remote Standard I/O	DeviceNet Unit	Master I/O data	Node	Output data	13)	• Communications Unit

5-8-3 Data Elements Set in Assemblies

Status Related Data

1) General Status

This is the status of the NE2A-series Controller.

Bit	Name	Status	Description
0	Overall Unit status	ON	Executing normal program. This bit is an AND of the following bits 1, 2, 3, 4, and 5
		OFF	There is an error, there is a connection that is not established, or a program has stopped.
1	I/O status	ON	Normal This bit will be ON if bits 0, 1, 2, 3, and 4 in *2) Error Status* are all OFF.
		OFF	Error
2	Safety I/O Communications status	ON	An AND of the I/O communications status for the Safety Master and the Safety Slave is given. • Safety Master: In normal execution or communications not set. • Safety Slave: In normal execution or communications not executed. ON if no Communications Unit is mounted.
		OFF	An AND of the I/O communications status for the Safety Master and the Safety Slave is given. • Safety Master: An error occurred or communications not executed. • Safety Slave: An error occurred.
3	Standard I/O Communications status	ON	An AND of the communications status of the DeviceNet Standard Master, DeviceNet Standard Slave, and EtherNet/IP tag data link target is given. • DeviceNet Standard Master: In normal operation or connection not set. • DeviceNet Standard Slave: In normal operation or communications not executed. • EtherNet/IP tag data link target: In normal operation or communications not executed. ON if no Communications Unit is mounted.
		OFF	An AND of the communications status of the DeviceNet Standard Master, DeviceNet Standard Slave, and EtherNet/IP tag data link target is given. • DeviceNet Standard Master: An error occurred or communications not executed. • DeviceNet Standard Slave: An error occurred. • EtherNet/IP tag data link target: An error occurred.
4	CPU Unit status	ON	Normal operation of CPU Unit. This bit will be ON if bits 7, 8, 9, and 10 in *2) Error Status* are all OFF.
		OFF	CPU Unit error detected.
5	Program execution status	ON	Normal execution of the program (RUN)
		OFF	Program execution is stopped or an error has occurred in program execution.
6	Reserved	OFF	
7	Reserved	OFF	

Bit	Name	Status	Description
8	RUN Mode status	ON	RUN Mode
		OFF	Not RUN Mode
9	Configuration lock status	ON	Locked. This bit turns ON when the Controller has a valid configuration and is already locked.
		OFF	Lock disabled or the Controller is not yet configured.
10	Forced status	ON	Force Mode is enabled. This bit turns ON when the Controller changes to Force Mode for a request from the Network Configurator.
		OFF	Force Mode is disabled.
11	Memory Card confirmation status	ON	A validated Memory Card is inserted
		OFF	A Memory Card is not inserted or the Memory Card has not been validated.
12 to 15	Reserved	OFF	---

2) Error Status

This is the error status of the NE2A-series Controllers.

Bit	Name	Status	Description
0	I/O Unit input power supply voltage error flag	ON	A voltage error occurred or power is OFF.
		OFF	There is no error or an I/O Unit is not mounted.
1	I/O Unit output power supply voltage error flag	ON	A voltage error occurred or power is OFF.
		OFF	There is no error or an I/O Unit is not mounted.
2	I/O Unit terminal error flag	ON	An error occurred.
		OFF	There is no error or an I/O Unit is not mounted.
3	Reserved	OFF	---
4	I/O Unit error flag	ON	An error occurred.
		OFF	There is no error or an I/O Unit is not mounted.
5	Safety I/O Communications error flag	ON	An error occurred. A communications error was detected on at least one Safety Master or Safety Slave connection.
		OFF	No error occurred or I/O communications are not being executed. This bit is turned OFF when a connection is not established.
6	Standard I/O Communications error flag	ON	An error occurred. A communications error was detected on at least one DeviceNet Master, DeviceNet Slave, or EtherNet/IP Tag Data Link connection.
		OFF	No error occurred or I/O communications are not being executed. This bit is turned OFF when a connection is not established.
7	Communications Unit error flag	ON	An error occurred. This flag indicates errors in data exchanges between the CPU Unit and Communications Units. It does not indicate errors in the Communications Units themselves. Errors in Communications Units are indicated in the Communications Unit status.
		OFF	No error occurred or no Communications Unit is mounted.
8	Parameter error flag	ON	An error occurred.
		OFF	An error has not occurred.
9	Setting error flag	ON	An error occurred.
		OFF	An error has not occurred.
10	System error flag	ON	An error occurred.
		OFF	An error has not occurred.

Bit	Name	Status	Description
11	Program execution error flag	ON	An error occurred. This flag is turned ON when an error occurs in one more function blocks.
		OFF	An error has not occurred.
12 to15	Reserved	OFF	---

3) Safety Connection Normal Status

This status indicates that the connection is normal for safety communications (Master and Slave). There is 1 bit per connection.

Bit	Connection ID	Status	Description
---	(Network No.) # Node address + Assembly data name	ON	Executing I/O communications
		OFF	I/O communications is not being executed or there is an error

Offset	D7	D6	D5	D4	D3	D2	D1	D0
0	#8	#7	#6	#5	#4	#3	#2	#1
1	#16	#15	#14	#13	#12	#11	#10	#9
	:	:	:	:	:	:	:	:
22	#184	#183	#182	#181	#180	#179	#178	#177
23	#192	#191	#190	#189	#188	#187	#186	#185

4) Safety Connection Error Status

This status indicates the connection error status for safety communications (Master and Slave). There is 1 bit per connection.

Bit	Connection ID	Status	Description
---	(Network No.) # Node address + Assembly data name	ON	I/O communications error
		OFF	I/O communications is not being executed or under normal operation.

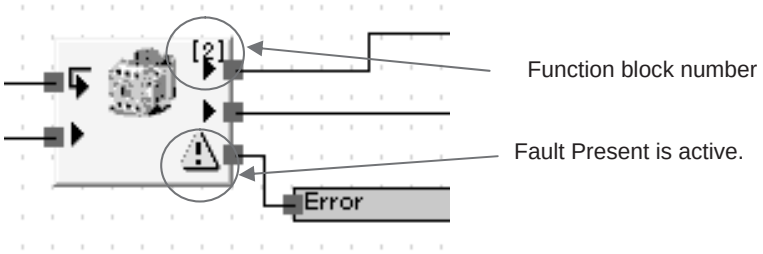
Offset	D7	D6	D5	D4	D3	D2	D1	D0
0	#8	#7	#6	#5	#4	#3	#2	#1
1	#16	#15	#14	#13	#12	#11	#10	#9
	:	:	:	:	:	:	:	:
22	#184	#183	#182	#181	#180	#179	#178	#177
23	#192	#191	#190	#189	#188	#187	#186	#185

5) Fault Present

A Fault Present Bit indicates whether there is a function block error. Each bit corresponds to a function block number. If the function bock does not have a logic function or if there is no fault present, the corresponding bit will be OFF. (The maximum number of registered function blocks is 1,600.)

Offset	D7	D6	D5	D4	D3	D2	D1	D0
0	#8	#7	#6	#5	#4	#3	#2	#1
1	#16	#15	#14	#13	#12	#11	#10	#9
	:	:	:	:	:	:	:	:
198	#1592	#1591	#1590	#1589	#1588	#1587	#1586	#1585
199	#1600	#1599	#1598	#1597	#1596	#1595	#1594	#1593

Bit	Name	Status	Description
---	Fault Present	ON	Indicates a function block error.
		OFF	Indicates a normal function block.



Note The function block number may change if the program is changed. When using a Fault Present signal as a fixed output from a program, use a variable name that is linked to the Fault Present Bit.

6) Safety Connection Communications Reopen Switch

This is a software switch for reopening the Safety Connection that was stopped by a communications error. There is 1 bit per connection. The connection will be re-established by turning ON the applicable bit from the user program. Once a switch is turned ON, the user program must be used to turn it OFF. The NE2A-series Controller reopens the Safety Network connection when this switch turns ON.

This switch can be used for Safety Master connections only. Bits that correspond to Safety Slave connections will be ignored even if they are turned ON.

Bit	Connection ID	Status	Description
---	(Network No.) # Node address + Assembly data name	ON	Reopens safety communications.
		OFF	Turn OFF from the program.

Offset	D7	D6	D5	D4	D3	D2	D1	D0
0	#8	#7	#6	#5	#4	#3	#2	#1
1	#16	#15	#14	#13	#12	#11	#10	#9
	:	:	:	:	:	:	:	:
22	#184	#183	#182	#181	#180	#179	#178	#177
23	#192	#191	#190	#189	#188	#187	#186	#185

Remote Standard I/O Related Data

7) DeviceNet Unit: DeviceNet Unit Status 1

Bit	Name	Status	Description
0	Error	ON	Indicates that an error related to the operation of the DeviceNet Unit has occurred. The bit turns ON if any of the Unit Status Bits from 1 to 15 is ON (an OR of bits 1 to 15).
		OFF	Indicates that the above error has not occurred, or the bit was turned OFF when the error was cleared.

Bit	Name	Status	Description
1	Master error	ON	Indicates that an error relating to the Master has occurred. (Refer to Master status 1.) The following errors can occur with the Master. • Verification error • I/O communications error • Incorrect scan list data • I/O refresh error
		OFF	Indicates that none of the above errors have occurred, or the bit was turned OFF when all the above errors were cleared.
2	Reserved	0	---
3	Slave error	ON	Indicates that at least one error relating to the Slave has occurred. (Refer to Slave status 1.) The following errors could occur with the Slave. • I/O communications error (for OUT1/IN1) • I/O communications error (for OUT2/IN2) • Illegal Slave setting • I/O refresh error
		OFF	Indicates that none of the above errors have occurred, or the bit was turned OFF when all the above errors were cleared.
4	Unit memory error	ON	Indicates that an EEPROM memory access (READ/WRITE) error has occurred.
		OFF	Indicates that the above error has not occurred. Once this error occurs, it will not return to a normal status. (It will remain ON.)
5	Bus Off detected	ON	Indicates that a Bus Off error occurred. When a Bus Off error occurs, the Unit goes offline and all communications operations will be stopped: scanning, Slave operation, and message communications.
		OFF	Indicates that the above error has not occurred. Once this error occurs it will not return to a normal status. (It will remain ON.)
6	Node address duplication	ON	Indicates that an error was found during the MAC ID duplication check when the Unit was started. If this occurs, the Unit will remain offline and all communications operations will be disabled.
		OFF	Indicates that the above error has not occurred. Once this error occurs it will not return to a normal status. (It will remain ON.)
7	Network power supply error	ON	Indicates that power is not supplied to the network.
		OFF	Indicates that the above error has not occurred, or the bit was turned OFF when the network power supply was re-applied.
8	Transmission timeout	ON	Indicates that the send request timed out. • There are no Slave Units. • The baud rate settings are different.
9 to 15	Reserved	OFF	---

DeviceNet Unit: DeviceNet Unit Status 2

bit	Name	Status	Description
0	Online	ON	Indicates that the Unit is online. The Unit will normally go online automatically but stays offline in the following situations. • Operation was stopped during the hardware or software check at Unit startup. • An error was found during the MAC ID duplication check.
		OFF	Indicates that the Unit is offline. The Unit will go offline when a Bus Off error occurs, turning OFF the bit.

bit	Name	Status	Description
1	Scan	ON	Indicates that the Master is scanning. The Unit will normally start scanning automatically but in the following situations it will not start. • No Slaves are registered in the scan list. • The scan list data is incorrect.
		OFF	Indicates that scanning has stopped. This bit will turn ON in the following situations to stop scanning. • An I/O communications error or a transmission error occurs while the stop scanning switch is ON. • The stop scan switch is set ON.
2	Operation switch change flag	ON	Indicates that a hardware switch setting was changed during operation. • Baud rate switch setting changed. • Node address switch setting changed. The flag will not change for changes in the unit number setting.
		OFF	No change in hardware switch settings. Or, the switch settings of the Communications Unit are changed during operation, and then the switch is returned to its previous settings.
3 to15	Reserved	OFF	---

8) DeviceNet Unit: DeviceNet Master Status

Bit	Name	Status	Description
0	Reserved	OFF	---
1	Reserved	OFF	---
2	I/O communications error	ON	Indicates that an I/O communications timeout has occurred between Slaves performing I/O communications.
		OFF	Indicates that an I/O communications error has not occurred, or that this bit was turned OFF when the I/O communications error was cleared.
3 to 14	Reserved	OFF	---
15	I/O communications	ON	Indicates that the Unit is performing I/O communications with one or more Slaves.
		OFF	The Unit is not performing I/O communications with the Slave.

9) DeviceNet Unit: DeviceNet Slave Status

Bit	Name	Status	Description
0	Reserved	OFF	---
1	Reserved	OFF	---
2	I/O communications error	ON	Indicates that a communications error occurred on at least one Slave I/O connection. This bit will not turn ON if there is a network power supply error or Busoff, or if the system goes offline.
		OFF	Indicates that an I/O communications error has not occurred, or that this bit was turned OFF when the I/O communications error was cleared.
3 to 14	Reserved	OFF	---
15	I/O communications	ON	Indicates that I/O communications is being performed correctly with the Master on an I/O connection. This bit turns ON when any one connection is established and then remains ON unless an error occurs.
		OFF	Indicates that I/O communications is not being performed correctly with the Master on the I/O connection (including idle status).

10) DeviceNet Unit: Registered Slave Table

This table indicates the Slaves communicating with the DeviceNet Master. Each bit corresponds to one DeviceNet node address.

This table is updated when the Unit is started or when a connection is registered.

Bit	Name	Status	Description
---	Registered Slave	ON	Indicates that the connection is registered.
		OFF	Indicates that the connection is not registered.

Offset	D7	D6	D5	D4	D3	D2	D1	D0
0	#7	#6	#5	#4	#3	#2	#1	#0
1	#15	#14	#13	#12	#11	#10	#9	#8
7	#55	#54	#53	#52	#51	#50	#49	#48
8	#63	#62	#61	#60	#59	#58	#57	#56

11) DeviceNet Unit: Normal Slave Table

This table indicates Slaves communicating with the DeviceNet Master. Each bit corresponds to one DeviceNet node address.

All bits are turned OFF when there is a communications power supply error, a transmission times out, or scanning stops (including scanning stopped by an error).

All bits will also turn ON if there is a communications error while using I/O communications and the Stop Scanning Setting Switch is ON. However, the I/O Communications Error Bit in the Slave Status will be turned ON for Slaves that caused scanning to stop.

Bit	Name	Status	Description
---	Normal Slave	ON	Indicates that a normal connection was established.
		OFF	Indicates all of the set connections could not be established.

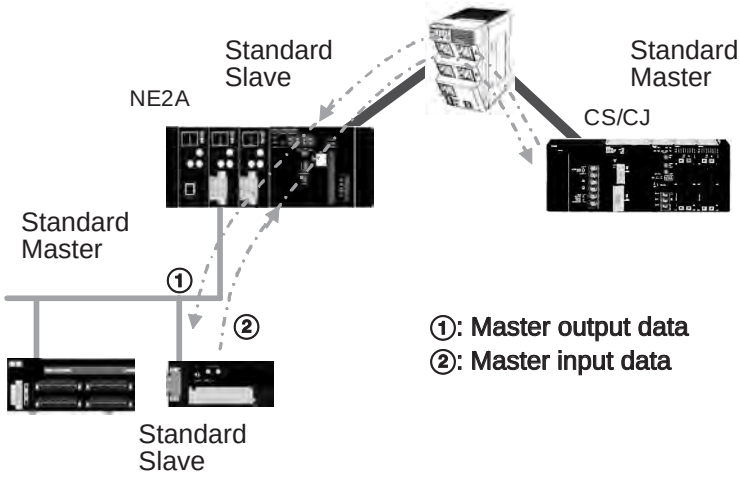
Offset	D7	D6	D5	D4	D3	D2	D1	D0
0	#7	#6	#5	#4	#3	#2	#1	#0
1	#15	#14	#13	#12	#11	#10	#9	#8
7	#55	#54	#53	#52	#51	#50	#49	#48
8	#63	#62	#61	#60	#59	#58	#57	#56

12) DeviceNet Master Output Data (NE2A to Slave)

This is output data that was 1) sent to a Slave that is set in the connection as the DeviceNet Standard Master, and then 2) received from the Standard Master. Each connection is allocated an area of 16 bytes.

13) DeviceNet Master Input Data (for Monitoring) (Slave to NE2A)

This is input data that was 1) received from a Slave that is set in the connection as the DeviceNet Standard Master, and then 2) sent to the Standard Master. Each connection is allocated an area of 16 bytes.



Note In Standard Communications, data can be transferred by assigning EtherNet/IP tag link data in the DeviceNet Master I/O data. Therefore, it is not necessary to write programming to copy data.

14) EtherNet/IP Unit: Unit Status 1

This is the status data for the EtherNet/IP Unit.

Bit	Name	Status	Description
0	Unit error	ON	Indicates that an error related to the operation for the EtherNet/IP Unit has occurred. The bit turns ON if any of the Unit Status Bits from 1 to 15 is ON (an OR of bits 1 to 15).
		OFF	Indicates that the above error has not occurred, or that the bit was turned OFF when the error was cleared.
1	Network error	ON	Indicates that at least one error related to the network has occurred. (Refer to the communications status.)
		OFF	Indicates that the above error has not occurred, or that the bit was turned OFF when the error was cleared.
2	Reserved	OFF	---
3	Reserved	OFF	---
4	Unit memory error	ON	Indicates that a Unit internal memory access (READ/WRITE) error has occurred.
		OFF	Indicates that the above error has not occurred. Once this error occurs it will not return to a normal status. (It will remain ON.)
5	Communications controller error	ON	Indicates that an error occurred in the Communications Controller.
		OFF	Indicates that the above error has not occurred. Once this bit has turned ON it will not turn OFF unless the power supply is cycled.
6	IP Address duplication error	ON	When the power supply is turned ON and every two minutes afterward, an ARP frame is sent to the ARP's local IP address. If there is a response, it is assumed that there is a duplicated address. Once this bit turns ON, it will not turn OFF unless the power supply is cycled or the Unit is restarted.
		OFF	This bit is OFF when there is no response to the above frames.
7	Reserved	OFF	---
8	Reserved	OFF	---
9	LINK OFF error	ON	A link with the hub was not established.
		OFF	A normal link was established with the hub.
10 to 15	Reserved	OFF	---

EtherNet/IP Unit: Unit Status 2

Bit	Name	Status	Description
0	Online	ON	Indicates that the Unit is online. This bit turns ON when explicit messages can be sent to the Ethernet. The Unit goes online after the IP duplication check is completed without any errors.
		OFF	Indicates that the Unit is offline • Error detected during hardware test after Unit is started. • IP address duplication error • Ethernet Communications Controller error (hardware error)
1	Reserved	OFF	---
2	Changing the IP address during operation	ON	This bit turns ON when the IP address is changed after the power supply is turned ON.
		OFF	In any situation other than the above.
3 to 14	Reserved	OFF	---
15	Error log	ON	Indicates that error log data is registered.
		OFF	Indicates that there are no errors registered in the error log. Also turns OFF when a request to clear the error log is received.

15) EtherNet/IP Unit: Communications Status 1

This is the EtherNet/IP Unit communications status data.

Bit	Name	Status	Description
0 to 2	Reserved	OFF	---
3	Tag Data Link (Standard I/O) Target connection error	ON	Indicates that there is an error on at least one Tag Data Link (Standard I/O) Target connection.
		OFF	Indicates that there are no errors on the Tag Data Link Target connection, or that this bit was turned OFF when the error on the Tag Data Link Target connection was cleared.
4 to 12	Reserved	OFF	---
13	Tag Data Link (Standard I/O) communication	ON	Indicates that at least one Tag Data Link (Standard I/O) connection is used in communications.
		OFF	In any situation other than the above.
14	Reserved	OFF	---
15	Reserved	OFF	---

EtherNet/IP Unit: Communications Status 2

Bit	Name	Status	Description
0 to 13	Reserved	OFF	---
14	Link status*1	ON	A link is established with the hub.
		OFF	The link with the hub is stopped.
15	Reserved	OFF	---

*1 This bit will have the opposite status of the LINK OFF error bit (bit 9 of EtherNet/IP Unit status 1).

EtherNet/IP Unit: Communications Status 3

Bit	Name	Status	Description
0	Reserved	OFF	---
1	Reserved	OFF	---
2	Ethernet basic settings error	ON	This bit turns ON when an error is found during the basic parameter check of the EtherNet/IP. This check if performed only when the power is ON.
		OFF	In any situation other than the above.

Bit	Name	Status	Description
3 to 8	Reserved	OFF	---
9	Ethernet advanced settings error	ON	This bit turns ON when an error is found during the advanced parameter check of the EtherNet/IP.
		OFF	In any situation other than the above.
10	BOOTP server error	ON	This bit turns ON when the following error occurs while using the BOOTP server. Illegal IP address received from the server. Timeout occurred in communications with the server
		OFF	In any situation other than the above.
11 to 14	Reserved	OFF	---
15	EEPROM error	ON	This bit turns ON when an EEPROM error occurs.
		OFF	This bit is turned OFF when EEPROM is operating normally.

Local I/O Data

16) Output Data

Safety Output Unit (NE2A-OD04-1)

This is the monitor data received from the Safety Output Unit. It is the output readback values.

Bit	Name	Status
0	Safety Output port readback #0	0: OFF 1: ON
1	Safety Output port readback #1	
2	Safety Output port readback #2	
3	Safety Output port readback #3	

17) Input Data

Safety Input Unit (NE2A-ID04-1)

This is the input data received from a Safety Input Unit. It is the value after single channel and dual channel evaluations.

Bit	Name	Status
0	Safety Input port #0	0: OFF 1: ON
1	Safety Input port #1	
2	Safety Input port #2	
3	Safety Input port #3	

18) Local I/O Status

Safety Output Unit (NE2A-OD04-1)

This is the terminal status of the Safety Output Unit. There is one bit per terminal.

Bit	Name	Status
0	Safety Output port status #0	0: Error 1: Normal
1	Safety Output port status #1	
2	Safety Output port status #2	
3	Safety Output port status #3	

Safety Input Unit (NE2A-ID04-1)

This is the terminal status of the Safety Input Unit. There is one bit per terminal.

Bit	Name	Status
0	Safety Input port status #0	0: Error 1: Normal
1	Safety Input port status #1	
2	Safety Input port status #2	
3	Safety Input port status #3	

19) I/O Unit Error Status

Safety Output Unit (NE2A-OD04-1)

This status data indicates the Safety Output Unit error status. There are 8 bits per Unit. The status is ON when there is an error and OFF during normal operation.

Bit	Name	Status	Description
0	Output power supply monitor flag	ON	Indicates the error status for I/O power supply voltage: Voltage Error or Power Supply OFF.
		OFF	Normal
1	Output port error flag	ON	Indicates that an output port error has occurred.
		OFF	Normal
2 to 15	Reserved	OFF	

Safety Input Unit (NE2A-ID04-1)

This status data indicates the Safety Input Unit error status. There are 8 bits per Unit. The status is ON when there is an error and OFF during normal operation.

Bit	Name	Status	Description
0	Input power supply monitor flag	ON	Indicates the error status for I/O power supply voltage: Voltage Error or Power Supply OFF.
		OFF	Normal
1	Input port error flag	ON	Indicates that an input port error has occurred.
		OFF	Normal
2 to 15	Reserved	OFF	

20) Local I/O Cause of Error

The cause of error for each I/O terminal of the Safety I/O Unit is displayed.

Offset	7	6	5	4	3	2	1	0
00000	Si1/So1				Si0/So0			
00001	Si3/So3				Si2/So2			

Safety Input Unit (NE2A-ID04-1)

Value (hex)	Description
00	No error
01	Incorrect configuration
02	Reserved
03	Safety Input terminal internal circuit error
04	Safety Input terminal discrepancy error
05	Error on other channel of dual channels

Safety Output Unit (NE2A-OD04-1)

Value (hex)	Description
00	No error
01	Incorrect configuration
02	Overcurrent detected at Safety Output terminal
03	Short-circuit detected at Safety Output terminal
04	Safety Output terminal fixed at high
05	Error on other channel of dual channels at Safety Output terminals
06	Reserved
07	Reserved
08	Data error between dual channel outputs at Safety Output terminals

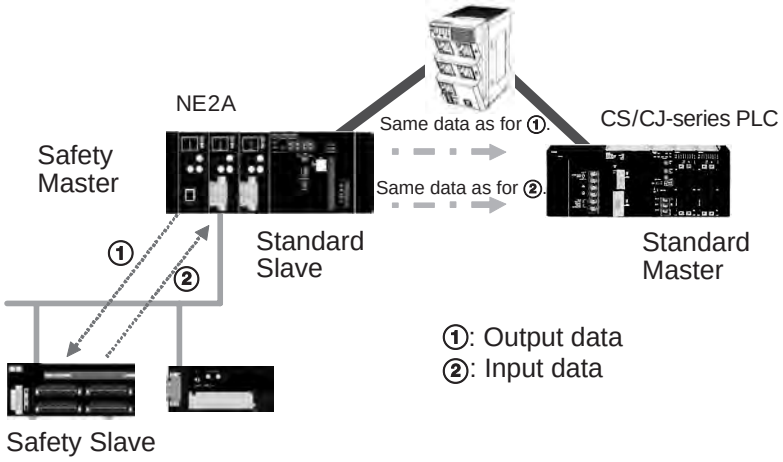
Remote Safety I/O Area

21) Output Data

This the same data as the output data that is sent to the Safety Slave that is set in a connection for which the NE2A-series Safety CPU Unit is set as the Safety Master. Each connection is allocated an area of 32 bytes.

22) Input Data

This the same data as the input data that is received from the Safety Slave that is set in a connection for which the NE2A-series Safety CPU Unit is set as the Safety Master. Each connection is allocated an area of 32 bytes.



5-9 Operation after a Communications Error

5-9-1 Data and Operation after a Communications Error

Data after a Communications Error

DeviceNet Safety Communications, EtherNet/IP Safety Communications, and DeviceNet Standard Communications:

- Input data from a Slave (Slave to NE2A) will be cleared if a communications error occurs in the Slave when the NE2A-series Controller is the Master.
- Output data from the Master (Master to NE2A) will be cleared if a communications error occurs with the Master when the NE2A-series Controller is the Slave.

EtherNet/IP Tag Data Links:

- Input data (Originator to NE2A) will be cleared if a communications error occurs with the Originator.

Setting the Operating Mode after a Communications Error

One of the following modes can be selected for the Safety Master when there is a connection timeout during Safety I/O Communications with the Safety Slave

This function is set for Safety Masters in each Communications Unit.

Mode after communications error	Description
Automatic recovery	Specify this mode to re-establish the Safety I/O connection after a Safety I/O Communications error has occurred. If the cause of the communications error is eliminated, Safety I/O Communications will restart automatically.
Stop only the connection where the error occurred.	Specify this mode to keep Safety I/O Communications stopped after a Safety I/O Communications error occurs on a connection. Communications on normal connections remain unaffected.Use one of the following methods to restart the stopped Safety I/O Communications. 1. Use the Network Configurator to send a command to restart communications. 2. Turn ON the Safety I/O Communications Restart Flag from the user program. Communications can be restarted with the specified trigger bit. The following two types of variables can be used. • Safety I/O Communications Status • Safety I/O Communications Restart Flag

5-10 Selecting the Ethernet Switching Hub

Note

- Always use a switching hub when using Safety Communications and Tag Data Links in the network.
- If a repeater hub is used for cyclic communications (i.e., Safety Communications and Tag Data Links), the network's communications load will increase, data collisions will occur frequently, and stable communications will not be possible.

5-10-1 Switching Hub Types

Layer 2 (L2) Switching Hub

These switching hubs use the Ethernet addresses to switch ports. Ordinary switching hubs have this function.

Layer 3 (L3) Switching Hubs

These switching hubs use the Ethernet or IP addresses to switch ports.

5-10-2 Switching Hub Functionality

This section describes the switching hub functionality that is important when using an EtherNet/IP network. Make a selection by dividing the switching hubs as follows according to functionality when using an EtherNet/IP Unit:

- L2 switching hub without multicast filtering
- L2 switching hub with multicast filtering
- L3 switching hub with multicast filtering and L4 QoS

Multicast Filtering

The multicast filter transfers multicast packets to the specific nodes only. This function is implemented in the switching hub as IGMP snooping or GMRP.

"Specific nodes" are the nodes that support an IGMP client that have made transfer requests to the switching hub. (NE2A-series Controllers and EtherNet/IP Units support an IGMP client.)

When the hub does not use multicast filtering, multicast packets are sent to all nodes, just like broadcast packets, which increases the traffic on the network.

Settings must be made in the switching hub to enable this function.

QoS (Quality of Service) for TCP/UDP Port Numbers

This function controls the priority of packet transmissions so that packets can be sent with higher priority to a particular IP addresses or TCP (UDP) port. The TCP and UDP protocols are called transport layer protocols, leading to the name L4 (layer 4) QoS.

When Safety Communications or Tag Data Links and message communications are executed on the same network, Tag Data Links can be sent at higher priority to prevent problems such as transmission delays due to message communications traffic and packet losses due to buffer overflow.

Settings must be made in the switching hub to enable this function and give higher priority to safety packets and Tag Data Link packets.

5-10-3 Precautions When Selecting a Switching Hub

The functionality supported by the switching hub may affect Tag Data Link transmission delays and the configuration. Select a switching hub based on the kind of communications that will be performed.

Selecting the Switching Hub Based on the Type of Network Communications

Executing Safety Communications or Tag Data Links

We recommend using an L2 switching hub without multicast filtering or an L2 switching hub with multicast filtering.

Using a switching hub with the multicast filtering prevents increased traffic due to unnecessary multicast packets, so the Safety Communications and Tag Data Links can operate at higher speed. If either of the following conditions exists, the amount of traffic will be the same for both kinds of switching hubs (with or without multicast filtering).

- The Safety Communications and Tag Data Links are set to share the same data with all nodes in the network. (The multicast packets are transferred to all nodes in the network just like broadcasting.)
- The safety communications and Tag Data Link settings are all one-to-one (unicast) and multicast packets cannot be used.

If the multicast filter function is being used, settings must be made for that function in the switching hub.

Mixed Execution of Safety Communications, Tag Data Links, and Message Communications

We recommend using an L3 switching hub with multicast filtering and L4 QoS.

By setting Safety Communications and Tag Data Link packets for higher-priority transmission, it is possible to prevent problems such as transmission delays due to message communications traffic and packet losses due to buffer overflow. Settings must be made in the switching hub when using the multicast filtering function and L4 QoS function.

- Ask the switching hub manufacturer for the setting procedures for the switching hub.
- Install the switching hub so that its environmental resistance capabilities are not exceeded.
  Ask the switching hub manufacturer for information on the environmental resistance of the switching hub.

SECTION 6
Local I/O Control Functions

The section describes the functions used to control local I/O in a NE2A-series Safety Network Controller.

6-1 NE2A-series Controller Local I/O Specifications. 140
6-2 Safety Input Functions 141
6-2-1 Outline 141
6-2-2 Setting the Channel Mode 141
6-2-3 Connecting Input Devices. 143
6-2-4 Setting a Dual Channel Mode. 147
6-2-5 Preventing the Effect of Chattering from External Devices 150
6-2-6 Error Handling 150
6-3 Safety Output Functions 152
6-3-1 Outline 152
6-3-2 Setting the Channel Mode 152
6-3-3 Wiring Output Devices 153
6-3-4 Dual Channel Channel Mode Setting 154
6-3-5 Error Handling 154

6-1 NE2A-series Controller Local I/O Specifications

A modular structure is used for local I/O for NE2A-series Controllers. A system with the optimal number of I/O points can be constructed because the number of local I/O points can be extended one I/O Unit at a time.

Number of Mounted Units and Maximum Number of Control Points

Up to 20 I/O Units (excluding the End Unit) can be mounted to an NE2A-series Controller.

The maximum numbers of local I/O control points for an NE2A-series Controllers are as follows:

- Safety Inputs: 80 points
- Test outputs: 40 points
- Safety Outputs: 80 points

Types of I/O Unit

Name	Model	Number of Units that can be connected
Safety Input Unit	NE2A-SID4-1	32
Safety Output Unit	NE2A-SOD4-1	

6-2 Safety Input Functions

6-2-1 Outline

The NE2A-SID4-1 Safety Input Unit provides four Safety Input terminals (Si0 to Si3) and two test output terminals (T0, T1).

Various applications can be supported by selecting settings and wiring that are appropriate for the types of input device that are connected and the safety level to be achieved.

Devices That Can Be Connected

The following table lists the devices that can be connected.

Devices	Examples
Safety Devices with mechanical contact outputs	Examples of Safety Devices with Mechanical Contact Outputs: Emergency Stop Switches, Safety Limit Switches, Safety Door Switches, Enable Switches, and Two-hand Switches
Safety Devices with semiconductor outputs	Examples of Semiconductor Output Safety Devices: Safety Light Curtains, Laser Scanners.
OMRON Safety Mats	UM **Note** Supports Safety Category 3.
OMRON D40A Non-contact Door Switches	D40A Supports Safety Category 3.
OMRON Single-beam Safety Sensors	E3FS/E3ZS **Note** Supports Safety Category 2.

6-2-2 Setting the Channel Mode

Set the channel mode for Safety Input terminals and the test output mode for test output terminals according to the external devices that are connected.

Setting the Channel Mode

Set the channel mode for the Safety Input terminals according to the external devices that are connected.

Channel mode	Description
Not Used	Specifies to not use an external device.
Used as Safety Input	Specifies connecting a Safety Device with a semiconductor output, such as a light curtain.
Test pulse from test out	Specifies connecting a Safety Device with a contact output in combination with a test output. Select a test output mode to use for the test source according to the Safety Device that is connected.

Setting the Test Output Mode

When the channel mode is set to *Test pulse from test out*, select the test output terminal used by the Safety Input as the test source.

Channel mode	Description
Mechanical contact	Pulses for diagnosing the Safety Devices will be output from the test output terminals. Pulses are output from each test output terminal at different timings. The Safety Input Unit's test output signal (pulse output) is input through the mechanical contact device. The following can be detected: Contact of the input signal line with the positive side of the power supply line, ground faults, and short circuits to the other input signal lines.
Single-beam Safety Sensor	A Single-beam Safety Sensor is connected. A test signal for Single-beam Safety Sensor diagnosis is output.
D40A Non-contact Switch	An OMRON D40A Non-contact Door Switch is connected. Test pulses for the D40A will be output.
Mat	A Safety Mat is connected. Test signals for diagnosing the Safety Mat will be output.

The following errors can be detected by using input circuit diagnosis and diagnosis of an externally connected device with test pulses from a test output terminal.

- Input circuit errors
- Externally connected device errors (including overcurrent detection and output ON error for test output terminals)

6-2-3 Connecting Input Devices

Connecting a Safety Device with a Contact Output

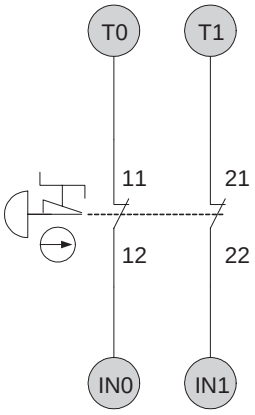
If the channel mode is set to *Test pulse from test output,* select *Mechanical contact* as the test output mode for the test output terminal.

The test output signal (a pulse output) is input to the input safety terminal through a contact output device. The following input signal line errors can be detected by inputting the test output signal.

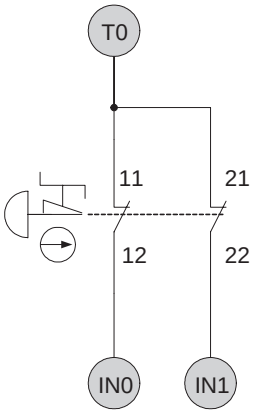
- Contact with the power supply line (positive side)
- Ground faults
- Short circuits between input signal lines

If detecting short circuits between input lines is necessary, specify a different test output terminal.

Examples:

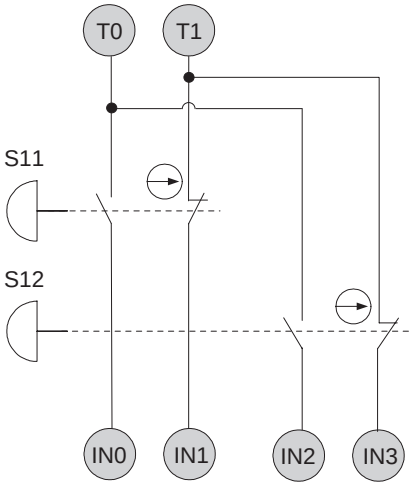


Circuit for Detecting Short Circuits between Input Signals



Circuit for Which Detecting Short Circuits between Input Signals Is Not Necessary

Example: Connecting to a Two-hand Switch



Note When connecting the switch, connect the NO terminals to IN0 and IN2, and connect the NC terminals to IN1 and IN3.

Connecting a Single-beam Safety Sensor

If the channel mode is set to *Test pulse from test output*, select *Single-beam Safety Sensor* as the test output mode for the test output terminal. A 24-VDC semiconductor output, such as an OSSD output from a Single-beam Safety Sensor, is input to the Safety Input terminal.

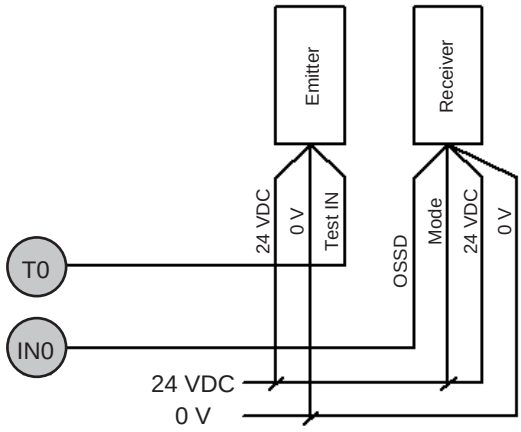
The following errors can be detected using the test output signal.

- Input signal contact with the power supply line (positive side)
- Ground faults of input signal
- Operation errors of externally connected device

The sensor is connected to input IN1.

■ Connecting a Single-beam Safety Sensor

Example:



Connecting a D40A Non-contact Switch

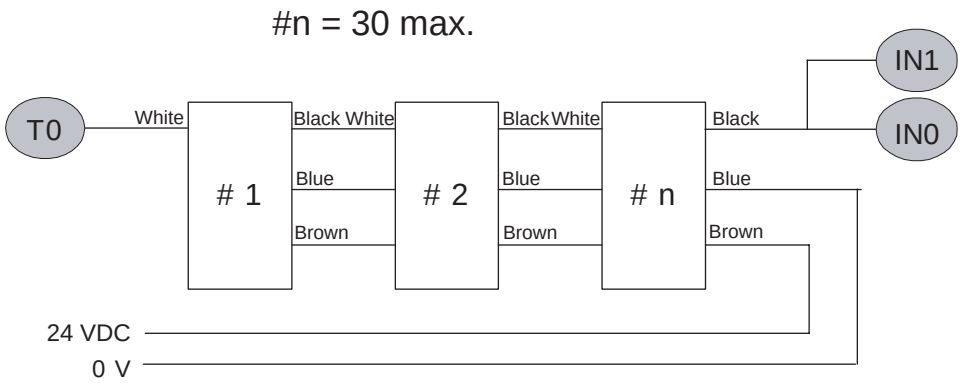
If the channel mode is set to *Test pulse from test output*, select *D40A Non-contact Switch* as the test output mode for the test output terminal. The OMRON D40A Non-contact Door Switch output is input to the Safety Input terminal.

The following errors can be detected using the test output signal.

- Input signal line contact with the power supply line (positive side)
- Ground faults of input signals
- Too many connected devices

■ Connecting an OMRON D40A Non-contact Door Switch

Example:



Note The OMRON D40A Non-contact Door Switch output is a single signal line. Create a branch from the Safety Input terminal (shown as IN0 and IN1 in the above diagram) to connect to the NE2A-SID4-1 Safety Input Unit.

Connecting a Safety Mat

If the input channel mode is set to *Test pulse from test output*, select *Mat* as the dual channel channel mode.

The Safety Mat output is input to the Safety Input terminal.

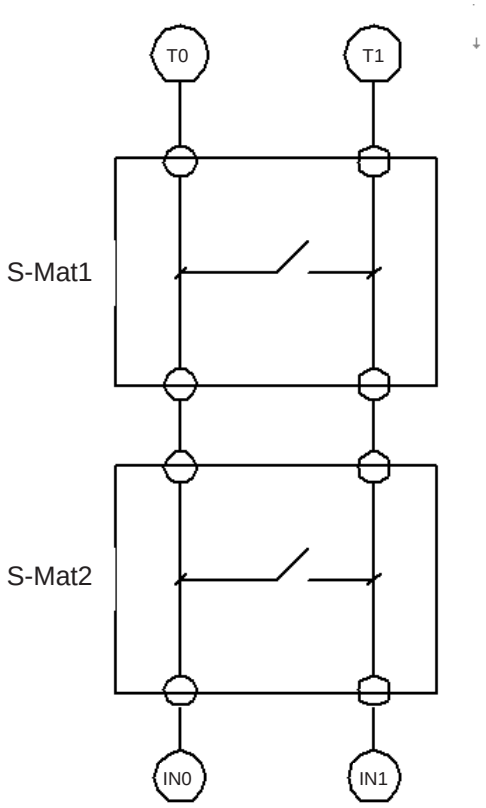
The following input signal line errors can be detected using the test output signal.

- Contact with the power supply line (positive side)
- Ground faults

Note Use Safety Input terminals Si0 and Si1 to connect a Safety Mat. A Safety Mat cannot be connected to Safety Input terminals Si2 and Si3.

■ Connecting a Safety Mat

Example:

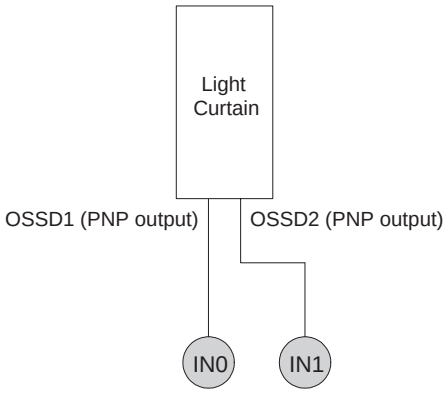


Connecting a Safety Device with a Semiconductor Output

Select *Used as Safety Input* as the input channel mode.

The output from a 24-VDC semiconductor, such as the OSSD output from a Light Curtain, is input.

Errors in the OSSD output signal line (i.e., the input signal line to the Safety Input Unit) are detected at the externally connected device.



6-2-4 Setting a Dual Channel Mode

Input safety terminals can be used as dual channels (one pair) for the NE2A-SID4-1 Safety Input Unit. Setting a Dual Channel Mode enables the following.

- Two inputs can be evaluated and the result reflected in a variable.
- The time difference between changes in status of the two Safety Input terminals (called the discrepancy time) can be evaluated. (This is not applicable to the MAT Dual Channel Mode.)

Channel mode	Description
Single Channel	The Safety Input terminals are used as independent Safety Input terminals.
Dual Channel Equivalent	The Safety Input terminals are used as a dual channel equivalent pair.
Dual Channel Complementary	The Safety Input terminals are used as a dual channel complementary pair.
MAT	The Safety Input terminals are used as Safety Mat Safety Input pair. This channel mode can be used for Safety Input terminals Si0 and Si1 only.

Saving Input Status in an Input Variable

The status input to the Safety Input terminals is saved in an input variable according to the dual channel mode, as shown in the following tables.

Dual channel channel mode	Input signal from input safety terminal	Input variable	Meaning of status
	Si (x)	IN (x)	
Single Channel	0	0	Inactive (OFF)
	1	1	Active (ON)

X = 0 to 3

Dual channel channel mode	Input signals from input safety terminals		Input variables		Meaning of status
	Si (x)	Si (n+1)	IN (n)	IN (n+1)	
Dual Channel Equivalent	0	0	0	0	Inactive (OFF)
	0	1	0	0	Discrepant status
	1	0	0	0	Discrepant status
	1	1	1	1	Active (ON)
Dual Channel Complementary	0	0	0	1	Discrepant status
	0	1	0	1	Inactive (OFF)
	1	0	1	0	Active (ON)
	1	1	0	1	Discrepant status

n = Even number

Dual channel channel mode	Status of Safety Mat	Input variables		Meaning of status
		IN0	IN1	
MAT	No load	1	1	Active (ON)
	With load	0	0	Inactive (OFF)

Discrepancy Time Evaluation

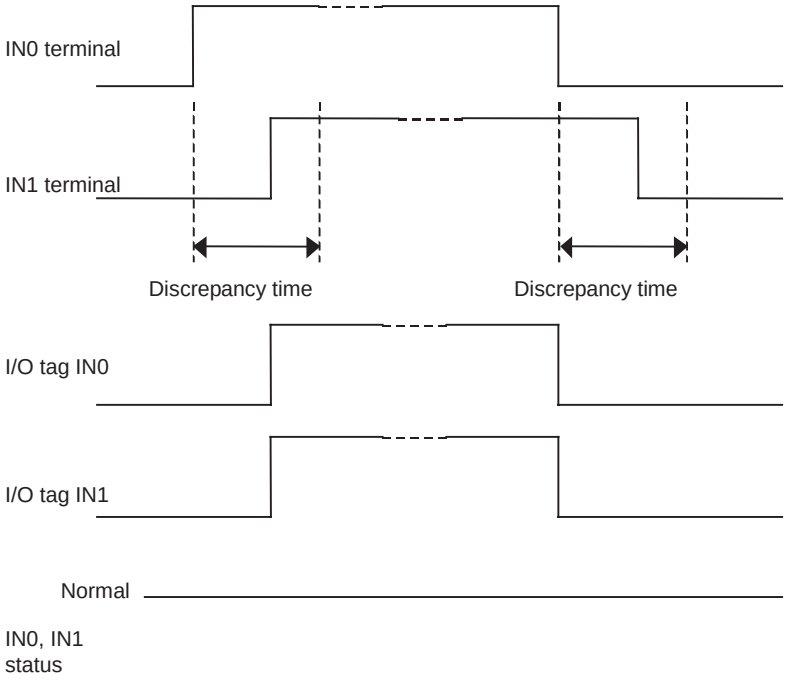
For two inputs set in a Dual Channel Mode, the time is monitored from a change in the value of one input to a change in the value of the other input (called the discrepancy time). An error occurs if the value of the other input does not change within the set discrepancy time.

The discrepancy time can be set in increments of 500 ms between 0 (disabled) and 63,500 ms.

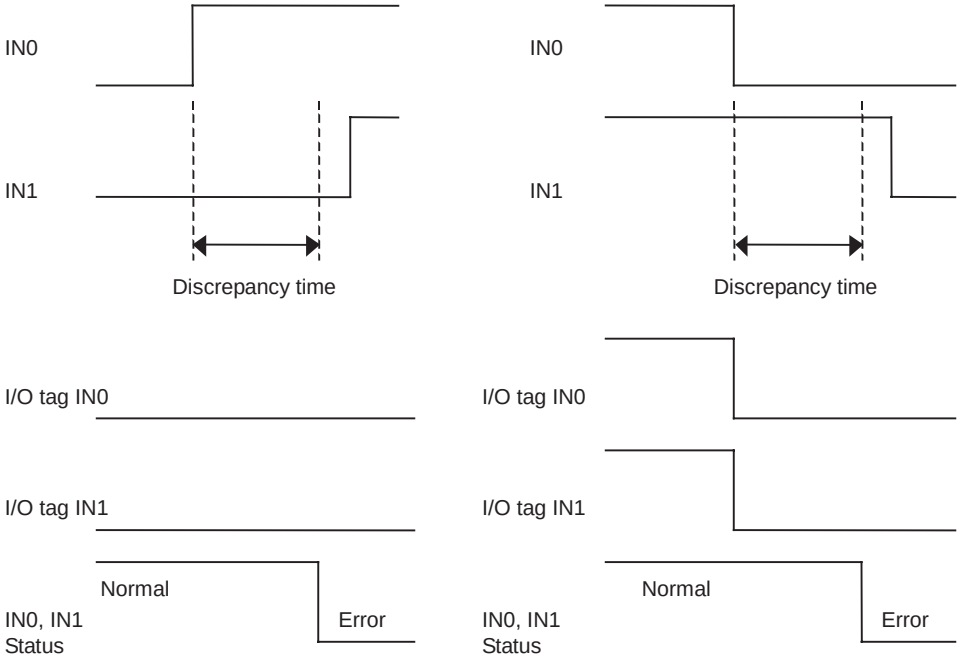
The discrepancy time cannot be set in Single Channel Mode.

Note Set the discrepancy time to 0 (disabled) when connecting an OMRON D40A Non-contact Door Switch so that disconnection of the Safety Input terminal will be detected.

Operation for Dual Channel Equivalent Inputs: Normal Operation



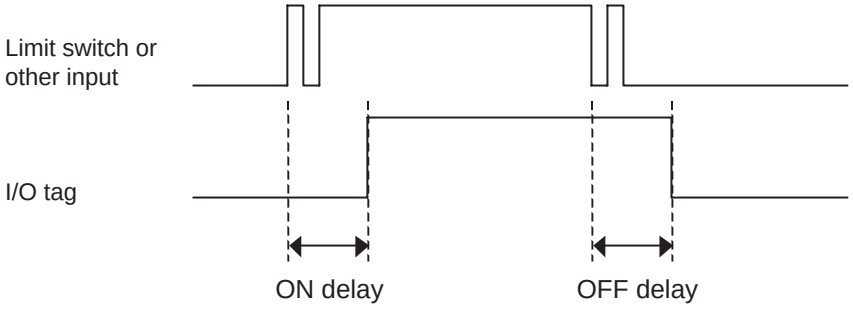
Operation for Dual Channel Equivalent Inputs: Discrepancy Error



6-2-5 Preventing the Effect of Chattering from External Devices

An input ON delay and OFF delay can be set between 0 and 1,024 ms for each input terminal. This helps prevent the effect of chattering from external devices connected to the Safety Input terminals.

The effect of chattering from external devices can be reduced more by increasing the delay value, but this will slow the response to input signals. The response will be faster if the delay value is made smaller, but this will increase the effect of chattering.



Note Delays will affect the safety response time and safety distance calculations. Be sure to add both the input ON delay and OFF delay to the I/O response performance.

6-2-6 Error Handling

Operation on Error Detection

Operation in Single Channel Mode

The following actions are performed if an error is detected during self-diagnosis.

- The variable corresponding to Safety Input for which an error has been detected is made inactive.
- The indicator of the Safety Input with the error lights red.
- The error appears in the error history.
- The NE2A-series Controller continues to operate.

Operation in a Dual Channel Mode

The following actions are performed if a discrepancy error is detected.

- The variables corresponding to Safety Inputs for which an error has been detected are made inactive.
- The indicators of both the Safety Input terminals with the error light red or go out.
- The error appears in the error history.
- The NE2A-series Controller continues to operate.

The following actions are performed if an error is detected in one of the two inputs.

- The variables corresponding to Safety Inputs for which an error has been detected are made inactive.
- The indicator of the Safety Input with the error lights red, and the indicator of the other input flashes red.
- The error appears in the error history.

- The NE2A-series Controller continues to operate.

Error Latch Time Setting

The error latch time can be set between 0 and 25,500 ms in increments of 100 ms. The default is 1,000 ms. When monitoring errors from a monitoring system, take the monitoring interval into account when setting the error latch time.

Error Latch Time:
The error latch time is the time to continue the error state when an error occurs. The error state will continue until the error latch time passes even if the cause of the error is removed immediately.

Resetting Errors

All the following conditions must be met to reset errors that occur in the Safety Inputs.

- The cause of the error must be removed.
- The latch error time must have lapsed.
- An inactive signal must be input (e.g., pressing the emergency stop button or opening a door).

6-3 Safety Output Functions

6-3-1 Outline

The NE2A-SOD4-1 Safety Output Unit provides four Safety Output terminals (So1 to So3). Various applications can be supported by selecting settings and wiring that are appropriate for the types of output device that are connected and the safety level to be achieved.

Devices That Can Be Connected

The following table lists the devices that can be connected.

Type	Example
Safety Devices with PNP output contacts	Safety relays and contactors

6-3-2 Setting the Channel Mode

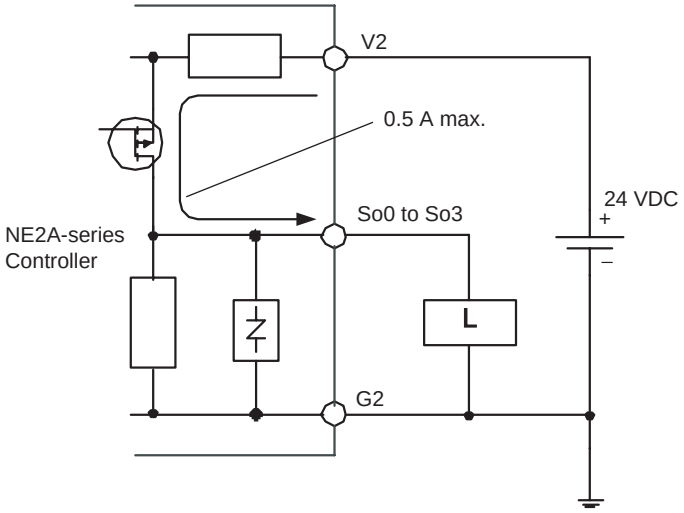
Set the channel mode for Safety Output terminals according to the external device that are connected. The following output signal line errors can be detected for the Safety Output terminals of the NE2A-SOD4-1 Safety Output Unit.

Channel mode	Description	Fault mode						
		Contact with the power supply line (positive side)		Ground faults		Short-circuits between output lines		
		Output when ON	Output when OFF	Output when ON	Output when OFF	Short-circuits between ON outputs	Short-circuits between OFF outputs	Short-circuits between ON and OFF outputs
Not Used	Not connected to an external output device.	---	---	---	---	---	---	---
Safety	Does not output test pulse when output is ON.	Not detect-able	Detect-able	Detect-able	Not detect-able	Not detect-able	Not detect-able	Detectable
Safety Pulse Test	Outputs test pulse when output is ON.	Detect-able	Detect-able	Detect-able	Not detect-able	Detectable	Not detect-able	Detectable

Note If *Safety Pulse Test* is set, an OFF pulse signal with a pulse width of 640 μs will be output to diagnose the output circuit when the Safety Output turns ON. Check the input response time of the control device connected to the NE2A-SOD4-1 Safety Output Unit to be sure that this OFF pulse will not cause malfunctions.

6-3-3 Wiring Output Devices

Refer to the following diagram to select and wire the output devices.



⚠ WARNING	
Serious injury may possibly occur due to breakdown of outputs. Do not connect loads beyond the rated value to the Safety Outputs and the test outputs.	
Serious injury may possibly occur due to loss of required safety functions. Wire the 24-VDC lines so that they do NOT touch the output lines and cause the load to turn ON when there is a short circuit.	
Serious injury may possibly occur due to loss of required safety functions. Ground the 0-V line of the power supply for external output devices so that the devices do not turn ON when the Safety Output line or the test output line is grounded.	
Serious injury may possibly occur due to loss of required safety functions. Use appropriate components or devices according to the requirements given in the following table.	

Control device	Requirements
Contactor	Use a contactor with a forcibly guided mechanism and NC contacts as a feedback signal to detect contactor failure. For feedback, use a device with NC contacts capable of switching micro-loads of 4 mA at 24 VDC.
Other control device	Evaluate whether the device is appropriate for the required safety category.

Note

- Do not use a cable that is longer than 3 m for the power supply.
- Be sure to separate I/O cables from high-voltage and power lines.
- Use I/O cables of 100 m or less.
- Do not apply power to the output terminals. Doing so may result in product damage or burning.

6-3-4 Dual Channel Channel Mode Setting

The NE2A-SOD4-1 Safety Output Unit can use Safety Outputs in a Dual Channel Mode. The following actions can be performed if a Dual Channel Mode is set:

- An error will occur if the two outputs from the user program are not equivalent.
- If an error is detected in either of the two output terminals, the outputs to the external devices are both turned OFF.

Channel mode	Description
Single Channel	The Safety Output terminals are used as independent Safety Outputs.
Dual Channel	The Safety Output terminals are used as a Dual Channel Safety Output pair. The output will turn ON if the paired Safety Output is normal.

Outputting the Status of the Output Variables to the Safety Output Terminals

The status of the output variable is output to the Safety Output terminals according to the channel mode, as shown in the following tables.

Dual channel channel mode	Output variable	Signal from output safety terminal	Meaning of status
	So (x)	OUT (x)	
Single Channel	0	0	Inactive (OFF)
	1	1	Active (ON)

X = 0 to 3

Dual channel channel mode	Output variable		Output signals from output safety terminals		Meaning of status
	So (n)	So (n+1)	OUT (n)	OUT (n+1)	
Dual Channel	0	0	0 (OFF)	0 (OFF)	Inactive (load OFF)
	0	1	0 (OFF)	0 (OFF)	Output data error (load OFF)
	1	0	0 (OFF)	0 (OFF)	Output data error (load OFF)
	1	1	1 (ON)	1 (ON)	Active

n = Even number

6-3-5 Error Handling

Operation on Error Detection

Operation in Single Channel Mode

The following actions are performed if an error is detected during self-diagnosis.

- The Safety Output for which a errors is detected is made inactive regardless of the status of the user program.
- The indicator of the Safety Output with the error lights red.
- The error appears in the error history.
- The NE2A-series Controller continues to operate.

Operation in a Dual Channel Mode

The following actions are performed if an error is detected in one of the two outputs.

- The outputs to external devices are immediately made inactive regardless of the status of the user program.
- The indicator of the Safety Output with the error lights red, and the indicator of the other output flashes red.
- The error appears in the error history.
- The NE2A-series Controller continues to operate.

The following actions are performed if the two outputs from the user program to the output variables are not equivalent.

- The outputs to the external devices are made inactive regardless of the status of the user program.
- The indicators of both of the Safety Output terminals with the error light red.
- The error appears in the error history.
- The NE2A-series Controller continues to operate.

Error Latch Time Setting

The error latch time can be set between 0 and 25,500 ms in increments of 100 ms. The default is 1,000 ms. When monitoring errors from a monitoring system, take the monitoring interval into account when setting the error latch time.

Resetting Errors

All the following conditions must be met to reset errors that occur in the Safety Outputs.

- The cause of the error must be removed.
- The latch error time must have elapsed.
- The output signal from the user application for the corresponding Safety Output terminal to the output variable must be inactive.

Note If a Dual Channel Mode is set for two outputs to implement redundant circuits and an error is detected for one of the outputs, the other output can be made to go inactive without relying on the user program. If redundant circuits are implemented using two outputs in Single Channel Mode, the user program must be used to detect the error using the External Device Monitoring function block.

SECTION 7
Functions for Operation and Maintenance

This section describes the functions used to operate and maintain a NE2A-series Safety Network Controller.

7-1 Access Control with Passwords 158
7-1-1 Project File Password 158
7-1-2 Parameter Passwords 158
7-1-3 Device Password 158
7-1-4 User-defined Function Block Passwords 159
7-1-5 Forgotten Passwords 159
7-2 Operation and Maintenance Using a Memory Card 161
7-2-1 Applications 161
7-2-2 Downloading Parameters and Locking the Configuration 161
7-2-3 Changing the Operating Mode 164
7-3 Examples of Security According to Roles 166

7-1 Access Control with Passwords

The NE2A System provides security to protect the user system and user assets from unintentional changes and access. Access to the following items can be controlled by setting passwords.

- Project files
- Parameters (includes programming)
- Devices
- User-defined function blocks

By using security and a Memory Card (see *7-2 Operation and Maintenance Using a Memory Card*), detailed security settings can be made that are suitable to the role of the NE2A-series Controller.

7-1-1 Project File Password

A password can be set for a project file to prevent unintentional changes.

Operations That Require a Project File Password

- Saving project files (Save/Save as)
- Downloading configurations after adding/deleting virtual networks
- Downloading configurations after adding devices to or deleting devices from virtual networks
- Changing the project file password
- Monitoring or force-setting and force-resetting bits on the Logic Editor

7-1-2 Parameter Passwords

Passwords for different operations can be set for NE2A-series Controller parameters (including programming). An access password can be set to authorize the use of the browse function and a modification password can be set to authorize changes to the parameters.

Operations That Require an Access Password

- Opening parameters, comparing parameters, and creating reports (including programming)
- Online monitoring of programs
- Force-setting/resetting variables

Operations That Require a Modification Password

- Changing parameters (including programming)
- Changing the parameter password or access rights

All of the operations that require an access password can be performed with the modification password.

7-1-3 Device Password

A device password can be set to prevent unintentional changes to the system in operation.

Operations That Require a Device Password

- Downloading parameters (including programming)
- Locking/Unlocking devices, changing between RUN and IDLE Mode, and restart operation

7-1-4 User-defined Function Block Passwords

Passwords and activation keys can be set for user-defined function blocks to prevent access or modifications.

Operating rights for user-defined functions blocks are shown in the following table.

		Editing	Access and monitoring	Importing
Password	**Modification**	Enabled	Enabled	Enabled
	Access	Disabled	Enabled	Enabled
Activation key		Disabled	Disabled	Enabled

Operations for Which an Access Password for User-defined Function Blocks Is Required

- Opening user-defined function blocks
- Online monitoring of user-defined function blocks
- Forced-setting/resetting
- Importing user-defined function blocks

Operations for Which a Modification Password for User-defined Function Blocks Is Required

- Changing user-defined function blocks
- Changing passwords

The access password for user-defined function blocks is sometimes also required.

Operations for Which an Activation Key Is Required

The activation key enables importing a user-defined function block for which an access or modification password is set.

The activation key can be confirmed when exporting a user-defined function block or when adding a user-defined function block to the library. It can also be confirmed from the menus of the Logic Editor.

7-1-5 Forgotten Passwords

Forgotten Device Passwords

If you forget a device password, contact your OMRON Support Center with the following information.

- Vendor ID
- Serial number
- Counter information

This information can be obtained by using the Password Recovery Tool installed in the Network Configurator.

If you enter the recovery key obtained from the Support Center in the Password Recovery Tool, you can return the device to the no-password setting.

For details, refer to *17-6-2 Lost Device Passwords*.

Forgotten Program Passwords

Passwords for the following items cannot be recovered if forgotten.

- Project files
- Parameters (including programming)
- User-defined function blocks

To use password protection, prepare and manage two files, one file with a password setting and another without a password.

Download the file with a password to the Safety Network Controller.

Note If you forget a password, the network configuration file can be opened only in read-only mode. You will not be able to edit the file.

7-2 Operation and Maintenance Using a Memory Card

By mounting a Memory Card that contains the Operation Rights File in the NE2A-series Controller, parameters and configuration locks can be set and the operating mode can be changed for CIP compatible devices on the same network within the system.

7-2-1 Applications

A Memory Card can be used for functions such as downloading parameters, locking the configuration, and changing the operating mode.

This enables the following functions without using the Network Configurator so that parameters and programming can be maintained in a black-box format. Also, there is no need to disclose the device password.

Constructing a System

Use these functions when constructing a new system.

Changing a System

Use these functions when changing the parameters or programming of an existing system.

Replacing a Faulty Device

Use these functions when replacing one or more faulty devices.

Changing the System Operating Mode

Use these functions to start and stop execution of the system program.

Operation Rights File

An Operation Rights File indicates whether the system status can be changed using the NE2A-series Controller functions. The file must be created with the Network Configurator and copied to a Memory Card before it can be used.

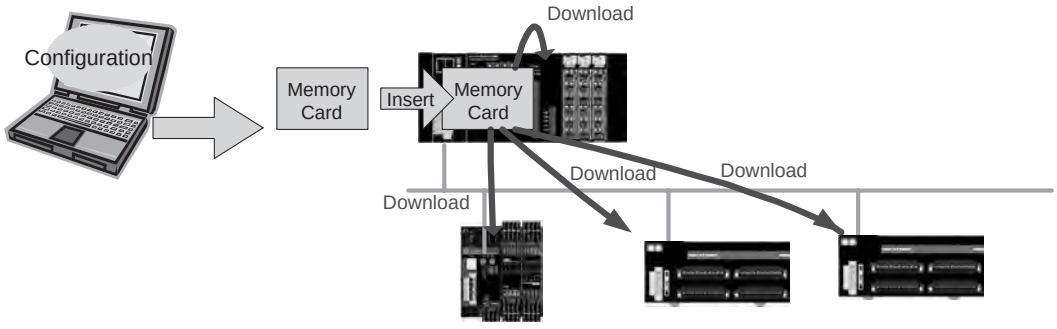
If the required information is stored in the Operation Rights File, parameters can be downloaded by the Memory Card and the operating mode can be changed for any NE2A-series Controller.

7-2-2 Downloading Parameters and Locking the Configuration

Downloading Parameters

Parameters for the following devices can be set using a Memory Card that contains an Operation Rights File.

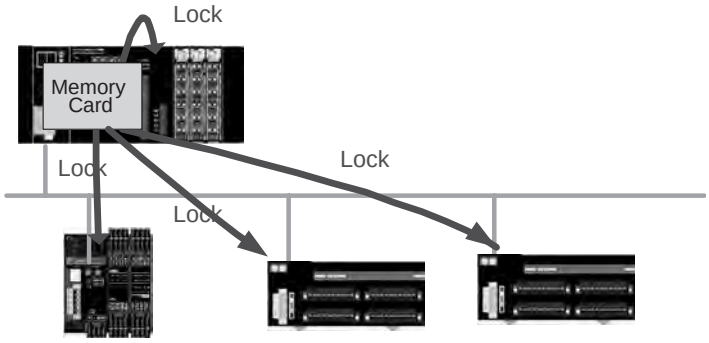
- The NE2A-Controller containing the Memory Card and all devices on the same DeviceNet networks (excluding NE2A-series Controllers)
- The NE2A-Controller containing the Memory Card



Locking the Configuration

The configuration of the parameters for the following devices can be locked using a Memory Card that contains the Operation Rights File.

- The NE2A-series Controller containing the Memory Card and devices on the same DeviceNet networks. (excluding NE2A-series Controllers)
- The NE2A-series Controller containing the Memory Card



Note To download or lock the configuration for an NE2A-series Controller, insert the Memory Card into the NE2A-series Controller. The configuration cannot be downloaded or locked for NE2A-series Controllers across a network or for Safety Devices that are connected through an ED Router.

Applicable Range

The following table shows the range of devices that are subject to downloading and locking by using a Memory Card.

The actual devices for downloading and locking within the applicable range are registered when the user creates the Operation Rights Files (devices that have parameters in the Memory Card). If only the local device is registered in the Operation Rights File, parameters are not downloaded and the configuration is not locked in the other devices in the applicable range.

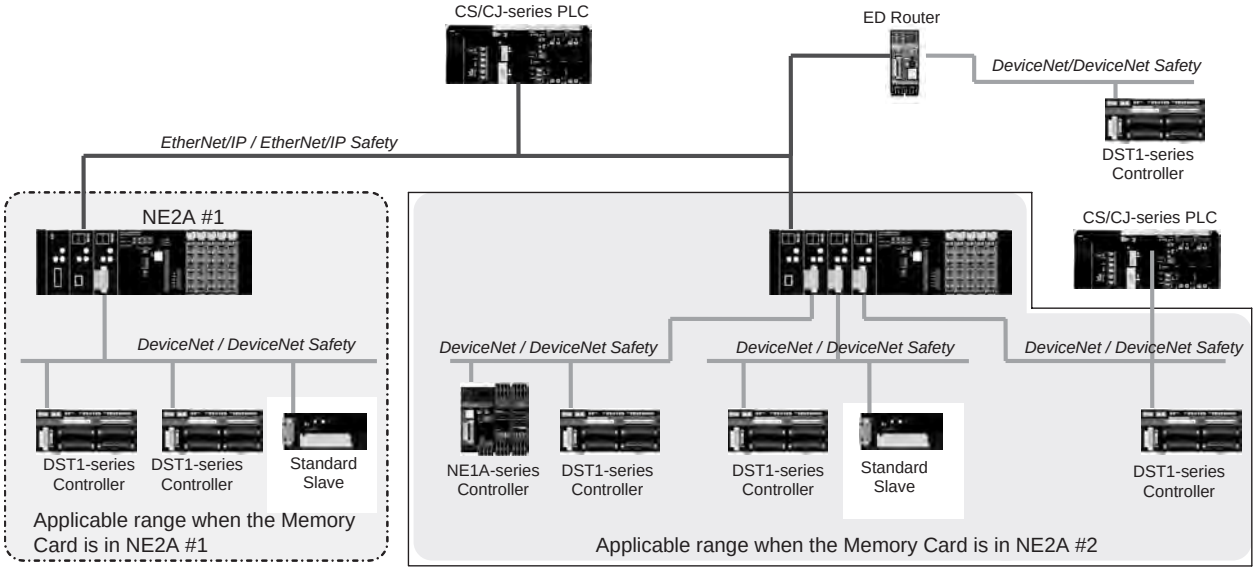
Device		Download from Memory Card	Lock by Memory Card
NE2A-series Controller containing the Memory Card	CPU Unit	Yes	Yes
	I/O Units	Yes	--
	DeviceNet Units	Yes	--
	EtherNet/IP Units	Yes	--
NE2A-series Controllers without the Memory Card	CPU Unit	No	No
	I/O Units	No	--
	DeviceNet Units	No	--
	EtherNet/IP Units	No	--
Safety Devices that are connected in the same DeviceNet network as the DeviceNet Unit	NE1A-series Controllers	Yes	Yes
	NE0A-series Controllers	Yes	Yes
	OMRON Safety Slaves that support safety communications	Yes	Yes
	OMRON Safety Slaves that do not support safety communications	Yes	Yes
Devices that are connected to a DeviceNet network that is connected through an ED Router		No	No

Device		Download from Memory Card	Lock by Memory Card
CS/CJ-series PLCs	CPU Unit	No	--
	DeviceNet Units	No	--
	EtherNet/IP Units	No	--
	Other Units	No	--
OMRON Standard Slaves		No	--

Yes: Subject to corresponding function, No: Not subject to the corresponding function, --: Locking not required.

Applicable Range Example

The following diagram shows the range of devices applicable to downloading and locking by the Memory Card. The range depends on the NE2A-series Controller that contains the Memory Card.



- If the Memory Card is in NE2A #1, downloading and locking can be performed for the Safety Devices on the DeviceNet network of the DeviceNet Unit in NE2A #1 (range indicated by dashed-dotted line).
- If the Memory Card is in NE2A #2, downloading and locking can be performed for devices on the DeviceNet networks of each DeviceNet Unit mounted to NE2A #2 (range indicated by solid line).

Restrictions

In the following two cases, parameter downloads and configuration locks by a Memory Card cannot be performed for a Target device. To use these functions, the Target device must be reset to default conditions. (Refer to *4-2-1 Resetting* for information on resetting the defaults.)

1. Downloading parameters that require the network number and node address to be changed
2. Replacing with a Safety Device that was used in a different system

Standard Devices are not subject to the restrictions mentioned above.

7-2-3 Changing the Operating Mode

The operating mode of the NE2A-series Controller can be changed from the Network Configurator or by using the RUN/STOP/RESTART switch on the CPU Unit. The RUN/STOP/RESTART switch is described in this section.

Program execution can be started, stopped, and restarted by using the RUN/STOP/RESTART switch on the NE2A-series CPU Unit. To use this function, a Memory Card that contains the Operation Rights File must be inserted in the NE2A-series CPU Unit.

When starting and stopping program execution, the applicable range can be changed using the NE2A-series System settings.

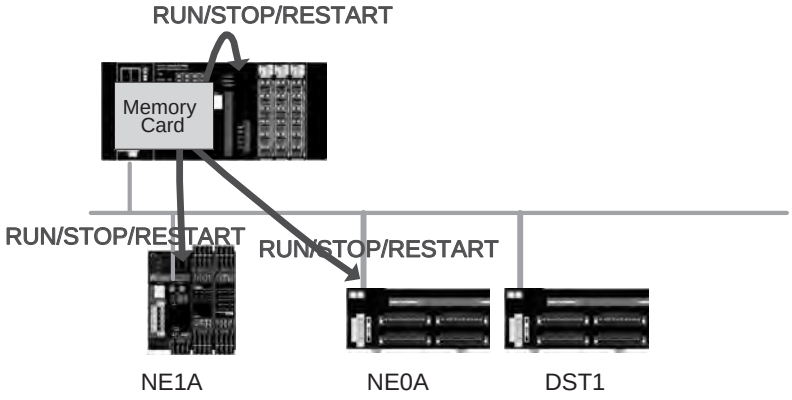
- Single NE2A-series Controller containing the Memory Card (default)
- The NE2A-series Controller containing the Memory Card and NE1A/NE0A-series Controllers on the same networks

The operating mode of the device can be changed by changing the switch only when the operating mode of the NE2A-series Controller and the switch position agree.

Example

If the switch is in the STOP position and the operating mode of the NE2A-series Controller is RUN, the operating mode of the device will not change even if the switch is changed from STOP to RUN.

The operating mode of the device will change when the switch is changed from STOP to RUN if the switch is in the STOP position and the operating mode of the NE2A-series Controller is STOP.



Starting, Stopping, Restarting NE2A-series Controller Program Execution

If the following conditions are satisfied, execution of the NE2A-series Controller program can be started, stopped, or restarted by using the RUN/STOP/RESTART switch.

- Only the NE2A-series Controller is set as the Target for starting, stopping, or restarting by the RUN/STOP/RESTART switch in the NE2A-series system settings (i.e., *Applicable to this device only* is set).
- The Memory Card that contains the Configuration Restore File is inserted and the user confirms that it is the correct Configuration Restore File.
- The configuration information of the NE1A/NE0A-series Controller that is set as the Target is included in the Configuration Restore File.

Starting and Stopping Execution of All NE□A-series Controllers on the Networks (Global Change)

The RUN/STOP/RESTART switch can be used to start or stop program execution of not only the NE2A-series Controller whose switch is operated, but also for the other NE1A-series, and NE0A-series Controllers on the same networks.

- Devices connected to the networks are set as the Targets for starting and stopping program execution by the RUN/STOP/RESTART switch in the NE2A-series system settings (i.e., *Applicable to all devices on the network* is set).
- A Memory Card that contains the Configuration Restore File is inserted and the user confirms that it is the correct Configuration Restore File.
- The configuration information of the NE1A/NE0A-series Controller that is set as the Target is included in the Configuration Restore File.

Note (1) Restarting program execution applies only to the NE2A-series Controllers. It cannot be applied globally.

(2) If the configuration restore function is also used, device replacement and system restarting can be performed without the Network Configurator.

Changing the Operating Mode with the RUN/STOP/RESTART Switch and Network Configurator

There is no priority between using the RUN/STOP/RESTART switch to start or stop program execution and changing the operating mode from the Network Configurator. Either way, program execution can be started or stopped at the desired time.

Check the status of the NE2A-series Controller program using the RUN indicator to determine if program execution is started or stopped. (Check the MS indicator for the operating mode.)

7-3 Examples of Security According to Roles

The following table lists the security functions and examples of the security achieved according to the roles.

		Operation																Means of achieving security
		Open a project file.	Save the project file.	Change the network configuration (add/delete).	Access log information and status information.	Open a device parameter (compare/create report).	Open a program.	Use program online monitor.	Force-set/reset variables in program.	Change a device parameter.	Change a program.	Change a device node address or baud rate.	Download a parameter.	Change device operation (lock/unlock/operating mode).	Change project file password.	Change parameter password and access rights.	Change device password. *1	
Device operation by Memory Card *1		No	No	No	No	No	No	No	No	No	No	No	OK	OK	No	No	No	
Operations requiring a device password		---	---	---	---	---	---	---	---	---	---	---	OK	OK	---	---	OK	
Operations requiring a parameter access password		---	---	---	---	OK	OK	OK	OK	No *2	No *2	---	---	---	---	No	---	
Operations requiring a parameter modification password		---	---	---	---	OK	OK	OK	OK	OK	OK	---	---	---	---	OK	---	
Operations requiring a project password		---	OK	OK *3	---	---	---	---	---	--- *3	--- *3	---	---	---	OK	---	---	
User classification	Operations enabled for operator that operates the machine	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	
	Operations enabled for maintenance person A Purpose: Device replacement only (Operation of NetworkConfigurator not required.)	No	No	No	No	No	No	No	No	No	No	No	OK	OK	No	No	No	• Allow Memory Card for restoration only
	Operations enabled for maintenance person B Purpose: Device replacement only (Maintenance using Network Configurator)	OK	No	No	OK	No	No	No	No	No	No	OK	OK	OK	No	No	OK	• Allow device password only
	Operations enabled for maintenance person C Purpose: Error investigation and device replacement	OK	No	No	OK	OK	OK	OK	OK	No	No	OK	OK	OK	No	No	OK	• Allow parameter access password • Allow device password
	Designer (manager)	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	• Allow all passwords

OK: Operation is enabled for correct password and disabled for incorrect password.

No: Operation is not possible. ---: Operation is not subject to protection.

*1 For Memory Card device operation, refer to *7-2 Operation and Maintenance Using a Memory Card*.

*2 The settings can be changed on the Network Configurator but they cannot be downloaded to the device.

*3 If the password is incorrect, the settings can be changed on the Network Configurator but they cannot be downloaded to the device.

*4 Refer to *17-6 Protecting Device Parameters*.

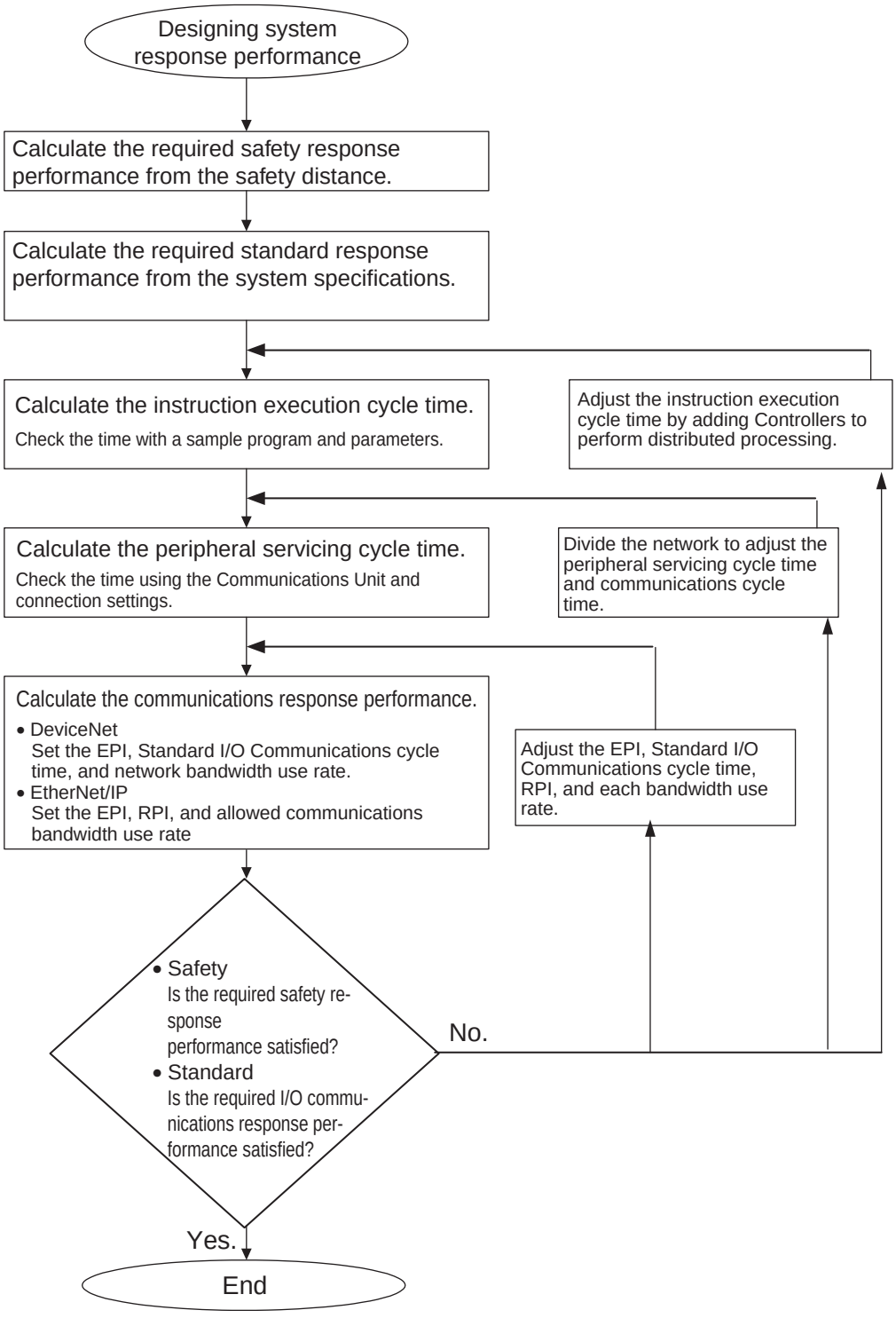
SECTION 8
Calculating System Performance

This section describes how to calculate the system performance, including the reaction time.

8-1 Calculating System Performance 170
8-2 Calculating Safety Response Performance 171
8-2-1 Reaction Time Concepts 171
8-2-2 Calculating the Reaction Time 171
8-3 Calculating Response Performance of Standard Communications. 177
8-3-1 Response Performance of DeviceNet Standard I/O Communications 177
8-3-2 Response Performance of EtherNet/IP Tag Data Link Communications 178
8-4 Calculating Cycle Times of NE2A-series Controllers 181
8-5 Calculating Communications Response Performance 183
8-5-1 Adjusting the DeviceNet EPI and Standard I/O Communications Cycle Time183
8-5-2 Adjusting EtherNet/IP EPI and RPI 185
8-5-3 Checking the Network Reaction Time 189
8-6 Checking and Adjusting the System Response Performance 191

8-1 Calculating System Performance

This section shows how to calculate system performance. The items to be considered for each step are described on later pages.



8-2 Calculating Safety Response Performance

Check that the reaction times satisfy the necessary specifications for all safety chains. If a reaction time exceeds the necessary specifications, reevaluate the system design so that the reaction time satisfies the necessary specifications.

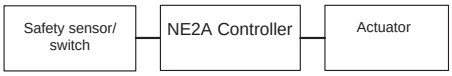
8-2-1 Reaction Time Concepts

The reaction time is the time required to stop machine operation in a worst-case scenario considering the occurrence of faults and failures in the safety chain.*1 The reaction time is used to calculate the safety distance.

*1 A safety chain is a logical connection to achieve safety functionality and consists of an input device, control device (which can be a remote I/O device), and an output device.

The reaction time is calculated for each safety chain. Some typical safety chains are shown below.

1. Local Input - Local Output



2. Remote Input - Local Output



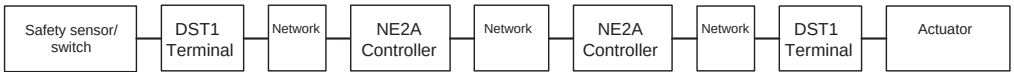
3. Local Input - Remote Output



4. Remote Input - Remote Output



5. Remote Input - Remote Output via Multiple Networks



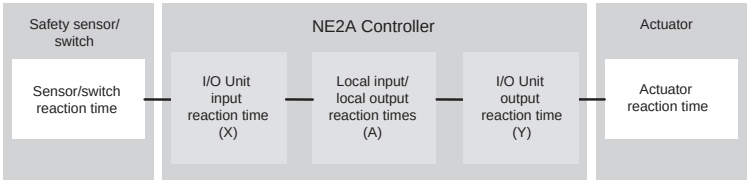
Note The reaction time is not the I/O reaction time when the system is operating normally. The reaction time must ensure that the output shutoff time will be maintained even if there are faults or failures in devices or the network.

8-2-2 Calculating the Reaction Time

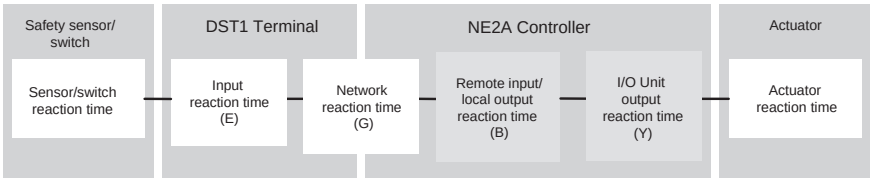
Elements of the Reaction Time

The elements of the reaction time are given below for each safety chain.

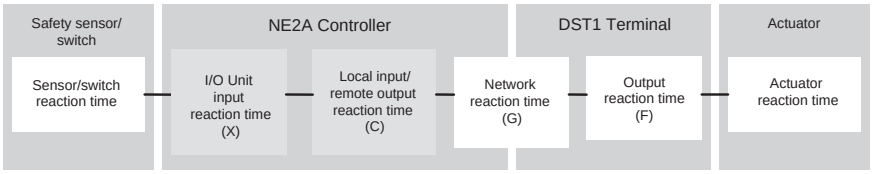
1. Local Input - Local Output



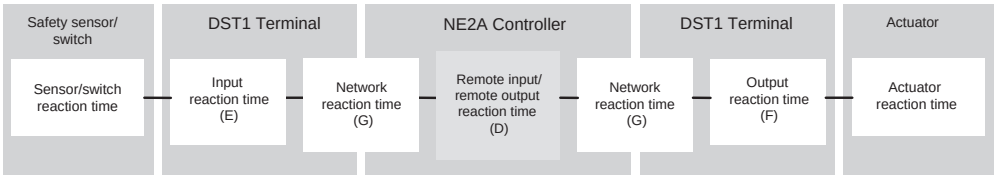
2. Remote Input - Local Output



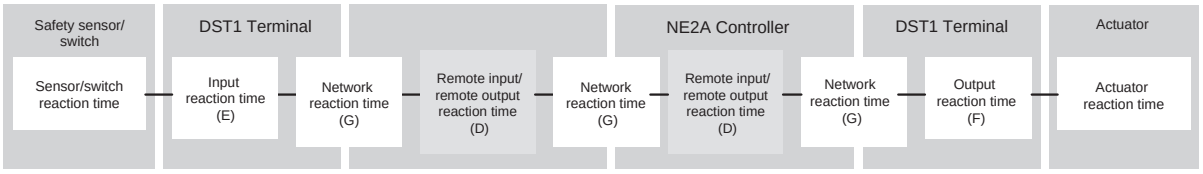
3. Local Input - Remote Output



4. Remote Input - Remote Output



5. Remote Input - Remote Output via Multiple Networks



Reaction Time Calculations

	Item	Calculation
A	Local input/local output reaction time (ms)	= Instruction execution cycle x 2 + 8.9 ms
B	Remote input/local output reaction time (ms)	= Instruction execution cycle x 2 + Peripheral servicing cycle + 3.9 ms
C	Local input/remote output reaction time (ms)	= Instruction execution cycle x 2 + Peripheral servicing cycle + 5.1 ms
D	Remote input/remote output reaction time (ms)	= Instruction execution cycle x 2 + Peripheral servicing cycle
E	Input reaction time (ms) of DST1-series Safety I/O Terminal	= ON/OFF delay + 16.2
F	Output reaction time (ms) of DST1-series Safety I/O Terminal	= 6.2 + Relay reaction time (DST1-MRD08SL-1 only)
G	Network reaction time (ms)*1	= Use the value calculated by the Network Configurator.
X	Input reaction time (ms) of Safety Input Unit	= ON/OFF delay + 2.3
Y	Output reaction time (ms) of Safety Output Unit	= 0.3

Refer to *8-4 Calculating Cycle Times of NE2A-series Controllers* for information on the instruction execution cycle and peripheral servicing cycle.

*1 Network Reaction Time
The network reaction time for Safety I/O Communications is not the same as the time required for normal communications. The network reaction time takes into consideration communications delays that can occur on the network. The network reaction time is calculated as follows:
The network reaction time between NE2A-series Controllers for a remote input to a remote output via multiple networks (refer to *Elements of the Reaction Time*, above) is as follows: EPI × 5
The reaction time for other configurations is as follows: EPI × 2 + Peripheral servicing cycle time × 3

Note If an output from a function block is fed back to the input side of the same function block, the instruction cycle time of the NE2A-series Controller must be added to the reaction time for the safety chain.

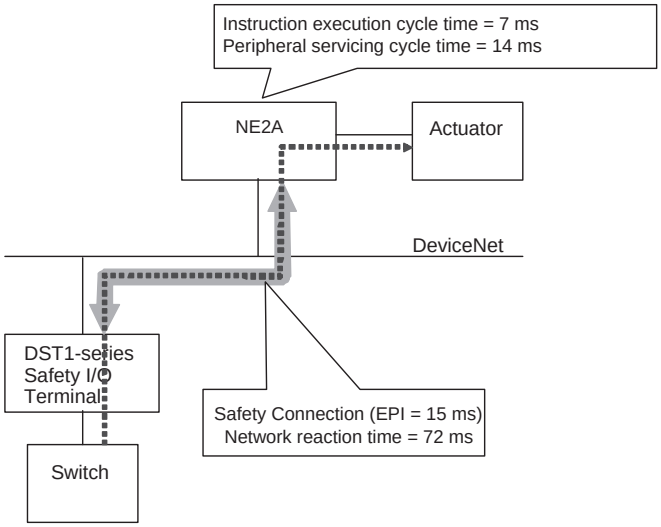
⚠ WARNING

Serious injury may possibly occur due to loss of required safety functions. Always confirm that the reaction time calculated for each safety chain satisfies the required specifications.



Reaction Time Calculation Examples

Example 1: Remote Input - NE2A-series Controller Output



The cycle times of the NE2A-series Controller read by the Network Configurator are as follows:

Instruction execution cycle time = 7 ms
Peripheral servicing cycle time = 14 ms

The network reaction time for the Safety Connection will be 72 ms.
The reaction time is obtained using the following equation:

Reaction time (ms) = Switch reaction time

+ DST1-series Safety I/O Terminal input reaction time

+ Network reaction time

+ NE2A-series Controller remote input/local output reaction time

+ Safety Output Unit reaction time

+ Actuator reaction time

= Switch reaction time

+ ON/OFF delay time (DST1-series Safety I/O terminal) + 16.2

+ 72

+ $7 \times 2 + 14 + 3.9$

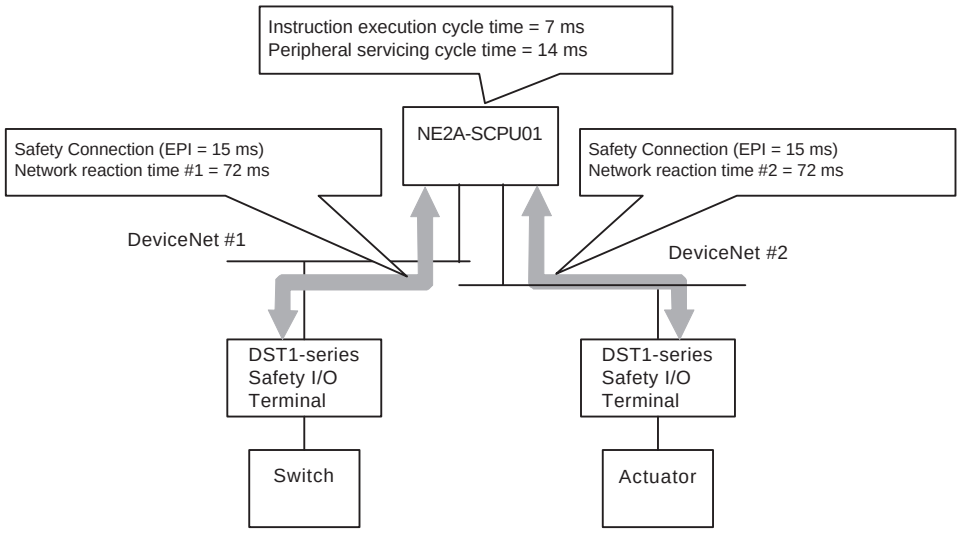
+ 0.3

+ Actuator reaction time

= 120.4 + ON/OFF delay time + Switch reaction time + Actuator reaction time

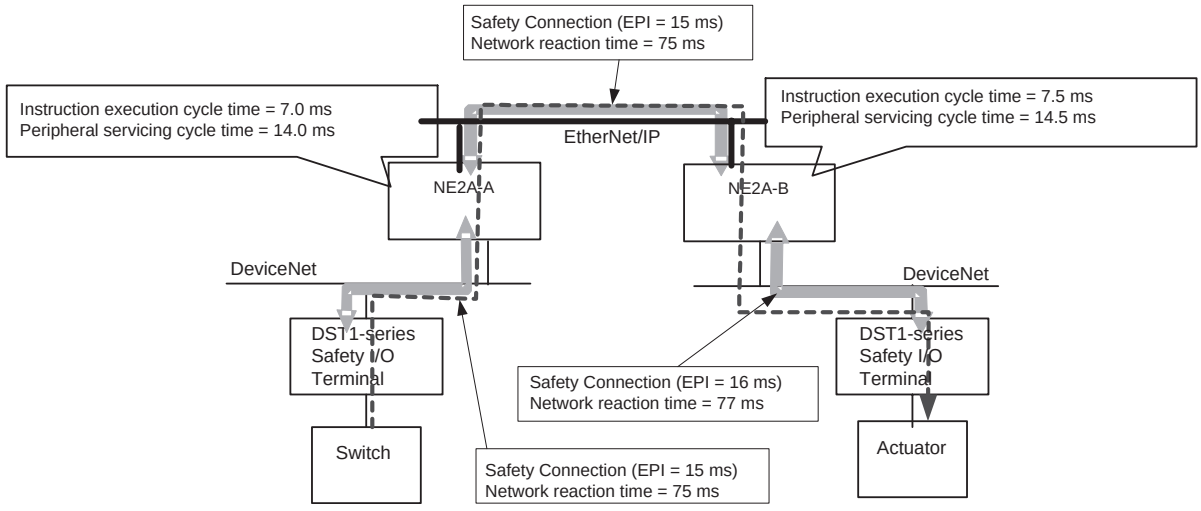
Example 2: Remote Input - Remote Output

In the following configuration, the DST1-series Safety I/O Terminals are on different DeviceNet networks, but calculations are the same as they would be if the DST1-series Safety I/O Terminals were on the same DeviceNet network.



Reaction time (ms) = Switch reaction time
+ DST1-series Safety I/O Terminal input reaction time
+ Network reaction time #1
+ NE2A-SCPU01 remote input/local output reaction time
+ Network reaction time #2
+ DST1-series Safety I/O Terminal output reaction time
+ Actuator reaction time #2
= Switch reaction time
+ ON/OFF delay time (DST1) + 16.2
(Input reaction time of DST1-ID12SL-1)
+ 72
+ 7 × 2 + 14
+ 72
+ 6.2 (= Output reaction time of DST1-MD16SL-1)
+ Actuator reaction time
= 194.4 + ON/OFF delay time + Switch reaction time + Actuator reaction time

Example 3: Remote Input - Remote Output (via Multiple Networks)



Reaction time (ms) = Switch reaction time
+ DST1-series Safety I/O Terminal input reaction time
+ Network reaction time
+ NE2A-series Controller remote input/remote output reaction time
+ Network reaction time
+ NE2A-series Controller remote input/remote output reaction time
+ Network reaction time
+ DST1-series Safety I/O Terminal output reaction time
+ Actuator reaction time
= Switch reaction time
+ 16.2 + ON/OFF delay (DST1-series Safety I/O Terminal)
+ 75
+ 7 × 2 + 14
+ 75
+ 7.5 × 2 + 14.5
+ 77
+ 6.2
+ Actuator reaction time
= 306.9 + ON/OFF delay + Switch reaction time + Actuator reaction time

8-3 Calculating Response Performance of Standard Communications

8-3-1 Response Performance of DeviceNet Standard I/O Communications

This section describes the performance of Standard I/O Communications when a DeviceNet Unit functioning as a Master and an OMRON Slave are used. Refer to this information if strict I/O timing is required.

The calculation shown here assumes that the following conditions are satisfied in the DeviceNet network:

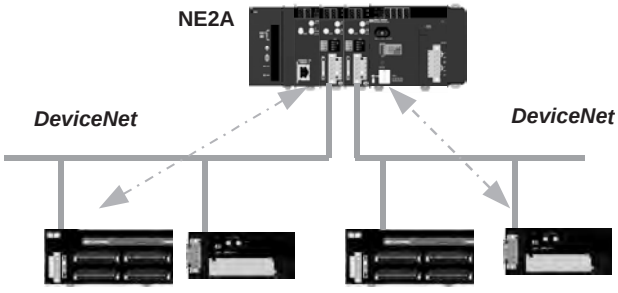
- All required Slaves are participating.
- There is no error displayed on the DeviceNet Unit.
- There is no message on the network occurring from a configurator made by another company.

Note

(1) The calculation results shown here may not match if the system also uses Masters or Slaves made by other companies.

(2) NE2A-series DeviceNet Units (NE2A-DNS21) do not have a Scan List Disabled Mode for Master operation. Therefore, it is necessary to register Slaves that will perform communications.

This section shows calculations for the maximum and minimum I/O response times in the following configuration.



Maximum I/O Response Time

The response time is calculated for the following delays.

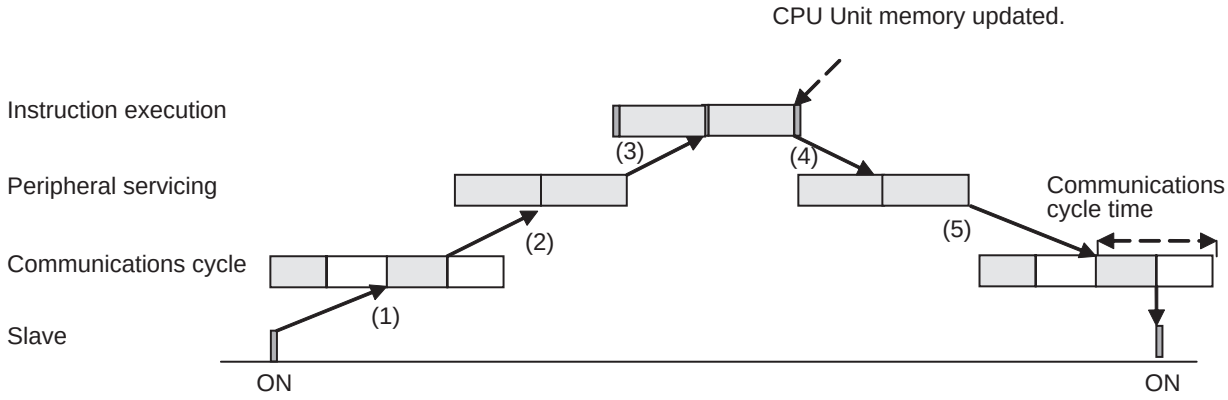
(1) The Slave input does not arrive in time for the DeviceNet communications cycle, and processing is delayed until the next DeviceNet communications cycle.

(2) The DeviceNet Unit reads the Slave input in the middle of peripheral servicing, and so processing is delayed until the next peripheral servicing cycle.

(3) The signal does not arrive in time to update the memory in the NE2A CPU Unit, and processing is delayed until the next time the memory is updated.

(4) The send data from the CPU Unit arrives in the middle of the peripheral servicing cycle, and processing is delayed until the next peripheral servicing cycle.

(5) The send data to the DeviceNet Unit does not arrive in time for the DeviceNet communications send cycle, and processing is delayed until the next DeviceNet communications cycle.

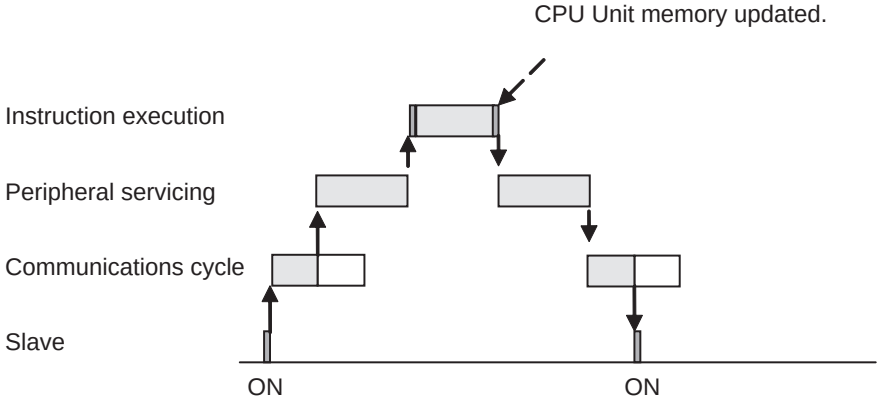


Maximum I/O response time = Input Slave ON (OFF) delay
+ Communications cycle time × 4
+ Peripheral servicing cycle time × 4
+ Instruction execution cycle time × 2
+ Output Slave ON (OFF) delay

Note Refer to the manual of the relevant Slave for information on the input Slave ON (OFF) delay and output Slave ON (OFF) delay.

Minimum I/O Response Time

The minimum I/O response time is calculated as the I/O response time when the communications cycle is executed immediately after input is read by the DeviceNet Unit.

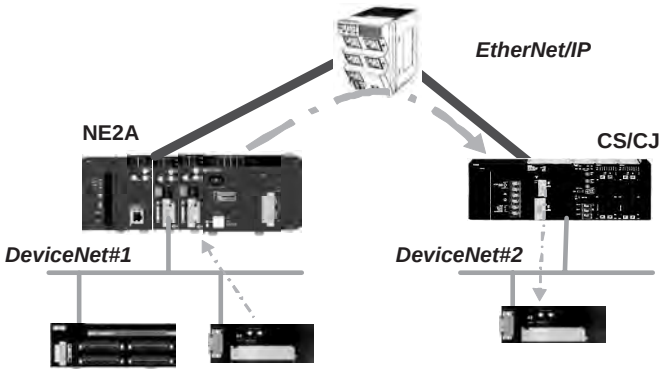


Minimum I/O response time = Input Slave ON (OFF) delay
+ Communications cycle time × 2
+ Peripheral servicing cycle time × 2
+ Instruction execution cycle time
+ Output Slave ON (OFF) delay

8-3-2 Response Performance of EtherNet/IP Tag Data Link Communications

This section describes the performance of Tag Data Link communications when an NE2A-series EtherNet/IP Unit, CJ/CS-series EtherNet/IP Unit, and Ethernet switching hub are used. Refer to this information if strict I/O timing is required.

This example shows how to calculate the minimum and maximum I/O response times for the following configuration.



Maximum I/O Response Time

The following delays occur.

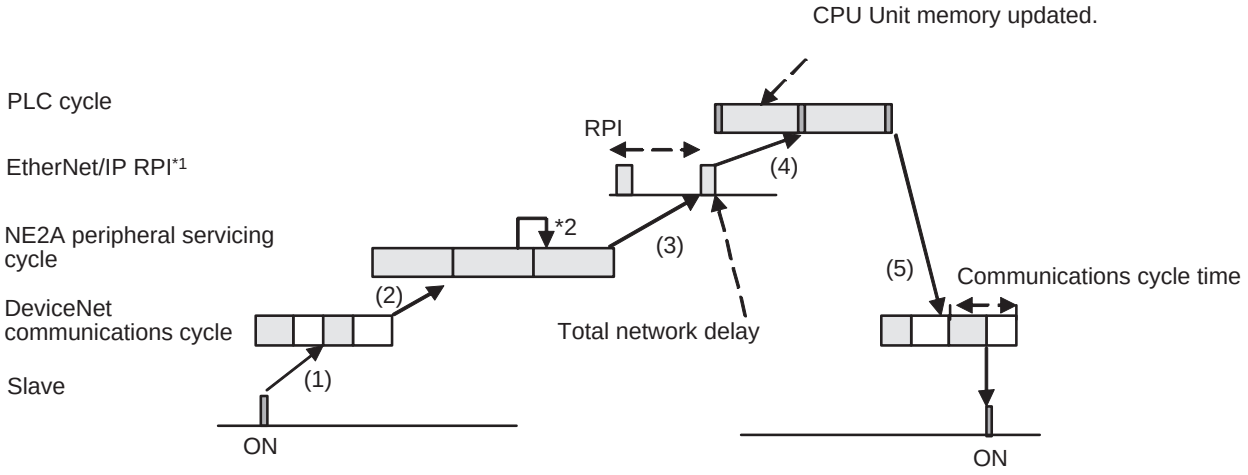
(1) The Slave input does not arrive in time for the DeviceNet communications cycle, and processing is delayed until the next DeviceNet communications cycle.

(2) The DeviceNet Unit reads the Slave input in the middle of NE2A peripheral servicing cycle, and so processing is delayed until the next NE2A peripheral servicing cycle.

(3) The send data to the EtherNet/IP Unit does not arrive in time to send the Tag Data Links, and processing is delayed until the next Tag Data Link. The total network delay is added to this interval.

(4) The signal does not arrive in time to update the receive data memory of the Standard PLC CPU Unit, and processing is delayed until the next PLC cycle time.

(5) The send data to the DeviceNet Unit does not arrive in time for the DeviceNet communications send cycle, and processing is delayed until the next DeviceNet communications cycle.



*1 The RPI (requested packet interval) is the interval of data communications in EtherNet/IP tag data link communications.

*2 With Standard Communications, data can be transferred by assigning DeviceNet Master input data (for monitoring) to EtherNet/IP Tag Data Link data.

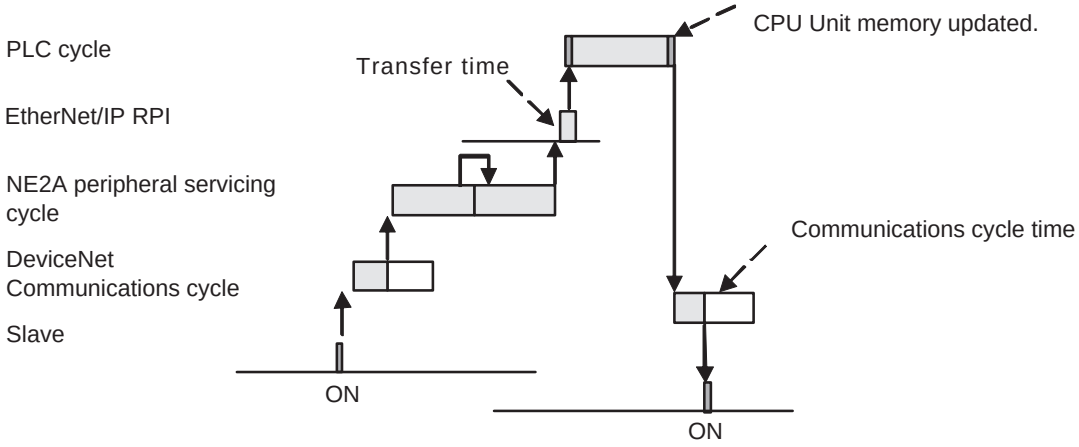
Maximum I/O response time = Input Slave ON (OFF) delay
+ DeviceNet #1 communications cycle time x 2
+ NE2A peripheral servicing cycle time × 3

+ EtherNet/IP RPI
+ Total network delay
+ PLC cycle time × 2
+ DeviceNet #2 communications cycle time x 2
+ Output Slave ON (OFF) delay

Note Refer to the manual of the relevant Slave for information on the input Slave ON (OFF) delay and output Slave ON (OFF) delay.

Note The I/O response time may increase due to noise or other factors.

Minimum I/O Response Time



Minimum I/O response time = Input Slave ON (OFF) delay
+ DeviceNet #1 communications cycle time
+ NE2A peripheral servicing cycle time × 2
+ Network delay *3
+ PLC cycle time
+ DeviceNet #2 communications cycle time
+ Output Slave ON (OFF) delay

*3 If no network delay occurs, only the data transmission time is totaled. Transmission time = (No. of transmission data bytes + 74) × 8 × 0.00001 (ms) (baud rate: 100 M/s)

8-4 Calculating Cycle Times of NE2A-series Controllers

The following three cycle times are used with an NE2A-series Controller.

Type	Description
Instruction execution cycle time	This time is mainly the cycle time for executing programming. The instruction execution cycle time for an NE2A-series Controller is automatically calculated according to the set parameters and programming. Values that are higher than the instruction execution cycle time are used for the ON-delay and OFF-delay settings.
Peripheral servicing cycle time	This time is mainly the cycle time for processing Communications Units (DeviceNet Units and EtherNet/IP Units) and USB communications. The peripheral servicing cycle time for the NE2A-series Controller is automatically calculated according to the number of Communications Units and the number of connections.

It is possible for the user to also set the instruction execution cycle time and peripheral servicing cycle time if the values are greater than the values calculated automatically by the Network Configurator.

By setting an extra margin in the values for the instruction execution cycle time and peripheral servicing cycle time that are calculated by the Network Configurator, it is possible to maintain a constant response performance (i.e., safety distance) to maintain constant cycle times even if the programming, parameters, or Communications Unit configuration change.
The following cycle times can be set:

- Instruction execution cycle time
  (Value calculated by the Network Configurator) to 50 ms (0.1-ms increments)
- Peripheral servicing cycle time
  (Value calculated by the Network Configurator) to 100 ms (0.1-ms increments)

Calculating the Instruction Execution Cycle Time

Complete the program and check the instruction execution cycle time by using the Network Configurator. If the program has not been completed, create a model program, and calculate the instruction execution cycle time from that program.

Calculating the Peripheral Servicing Cycle Time

Make the Communications Unit and connections and check the peripheral servicing cycle time using the Network Configurator.

Checking Cycle Times

With an NE2A-series Controller, you can check the instruction execution cycle time and peripheral servicing cycle time by using the Network Configurator.



IMPORTANT The user has to define the maximum allowed values, depending on his safety application, which are entered in the input box.

8-5 Calculating Communications Response Performance

The value required in the network reaction time is determined from the calculated reaction time (safety response performance). The values required in the Standard I/O Communications cycle time and RPI are determined by the calculated standard response performance.

This section describes how to calculate the network reaction time, EPI, Standard I/O Communications cycle time, and RPI. The EPI, communications cycle time, and RPI affect the calculation of network reaction time.

8-5-1 Adjusting the DeviceNet EPI and Standard I/O Communications Cycle Time

The DeviceNet EPI (expected packet interval) and Standard I/O Communications cycle time affect the network bandwidth usage (*1) used in Safety I/O Communications and Standard I/O Communications. The performance of the EPI and Standard I/O Communications cycle time can be adjusted by adjusting the network bandwidth usage used in Safety I/O and Standard I/O Communications.

*1 Network Bandwidth Usage
Shortening the EPI and Standard I/O Communications cycle time increases the network bandwidth usage. Conversely, lengthening the EPI and Standard I/O Communications cycle time decreases the network bandwidth usage.

With DeviceNet, it is possible to use approximately 90% of the network bandwidth for either Safety I/O Communications or Standard I/O Communications. Communications will time out, however, if a connection is set that exceeds the network bandwidth usage for Safety I/O Communications or Standard I/O Communications. Therefore, it is necessary to set the EPI and Standard I/O Communications cycle time so that the network bandwidth usage is not exceeded.

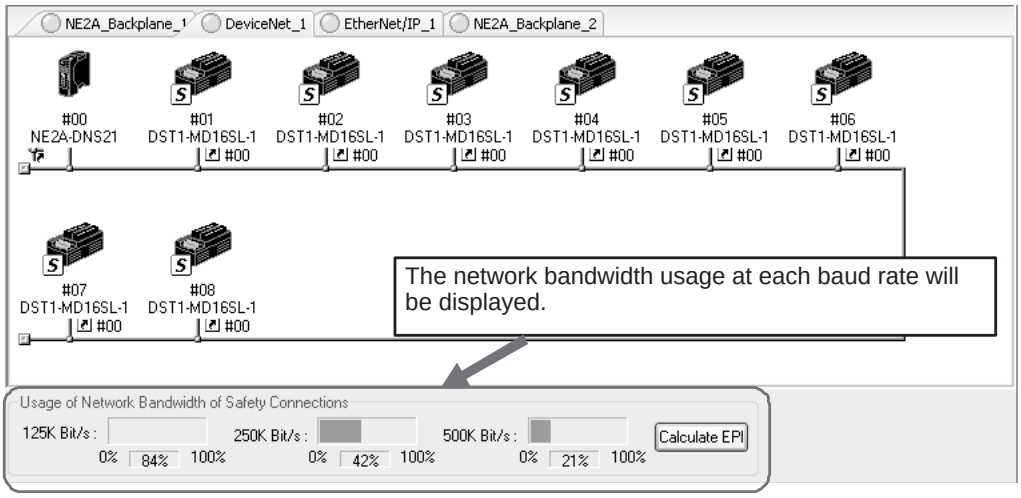
Note
(1) For details on EPI, refer to *5-4-2 Setting Safety Connections*.
(2) For details on the Standard I/O Communications cycle time, refer to *5-5-2 Standard Connection Settings*.

Checking the EPI and Standard I/O Communications Cycle Time Settings and Network Bandwidth Usage

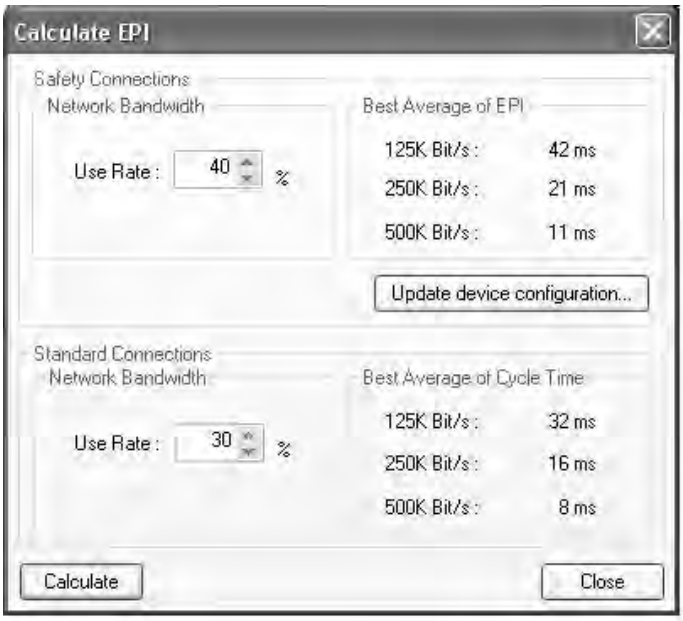
The best EPI and best Standard I/O Communications cycle times for Safety I/O Communications and Standard I/O Communications can be calculated by inputting the network bandwidth usage for Safety I/O Communications and the network bandwidth usage for Standard I/O Communications in the Network Configurator.

It is necessary to check the EPI, Standard I/O Communications cycle time, and network bandwidth usage for each network.

The network bandwidth usage will be calculated for each baud rate when a Safety Connection or Standard Connection is set.



The EPI and Standard I/O Communications cycle time will be automatically calculated if you set the use rate for the Safety Connections and Standard Connections in the Calculate EPI Dialog Box.



Note The status of network bandwidth usage shows the total bandwidth usage for Safety Connections and Standard Connections.

Changing the EPI Settings of Safety I/O Connections

The best average EPI calculated by the Network Configurator is the average value for all Safety Connections. Adjust the overall network EPI such as in the following examples. If a connection requires a high-speed reaction time, such as to connect a safety curtain, decrease the EPI. If high speed is not required, such as to connect a door switch in a non-hazardous area, increase the EPI.

8-5-2 Adjusting EtherNet/IP EPI and RPI

By using full-duplex communications and an EtherNet switching hub, EtherNet/IP enables allocating network bandwidth for individual nodes rather than sharing the network bandwidth with all nodes. Communications can be performed at high speed and with stability because the nodes are not affected by the communications load on other nodes, and so collisions do not occur.

The allowed Unit communications bandwidth (*1) is one restriction on the performance of safety I/O communications and tag data link communications for EtherNet/IP. Shortening the EPI or RPI increases the allowed Unit bandwidth usage. Conversely, lengthening the EPI or RPI decreases the allowed Unit bandwidth usage.

Each type of communications will time out, however, if a connection is set that exceeds the network bandwidth usage in each type of communications. Therefore, it is necessary to set the EPI and RPI so that the allowed Unit communications bandwidth is not exceeded.

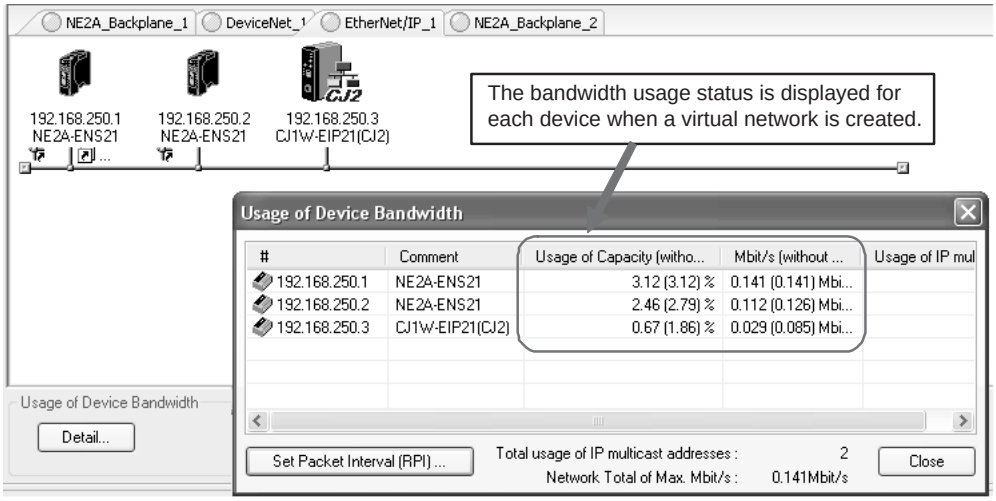
*1 For details on the allowed Unit communications bandwidth, refer to the next page.

Note (1) For details on the EPI, refer to *5-4-2 Setting Safety Connections.*

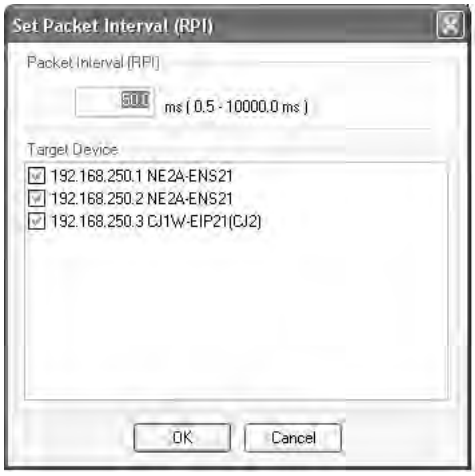
(2) For details on the RPI, refer to *5-7-2 Setting Tag Data Link Connections*.

EPI and RPI Settings and Allowed Unit Communications Bandwidth Usage

When the safety connection and tag data link connection are set, the allowed Unit bandwidth usage will be calculated for each device. The EPI, RPI, and allowed Unit communications bandwidth must be check for each network.



You can set the packet interval (RPI) for the Tag Data Links in the Set Packet Interval (RPI) Dialog Box.



Allowed Unit Communications Bandwidth for EtherNet/IP Units

The number of packets that the Unit can transfer in one second in EtherNet/IP Safety Communications and Tag Data Links is called the allowed Unit communications bandwidth, or packets per second (PPS). The maximum number of packets that an NE2A-ENS21 Unit (hereafter, EtherNet/IP Unit) can send or receive in one second (i.e., the allowed communications bandwidth) is 6,000 pps. Make the connection settings within this range.

The PPS is calculated for each EtherNet/IP connection from the EPI and RPI by using the following equations.

PPS value (pps) used in Safety Connection = 1,000 ÷ EPI (ms)
PPS value (pps) used in Tag Data Link connection = 1,000 ÷ RPI (ms)

The total number of packets sent or received in one second by each EtherNet/IP Unit is calculated by using the following equation.

Total PPS for EtherNet/IP Units = Total PPS for Safety Master connections
+ Total PPS for Safety Slave connections
+ Total PPS for Originator connections
+ Total PPS for Target connections

Example:

Node 1 has:

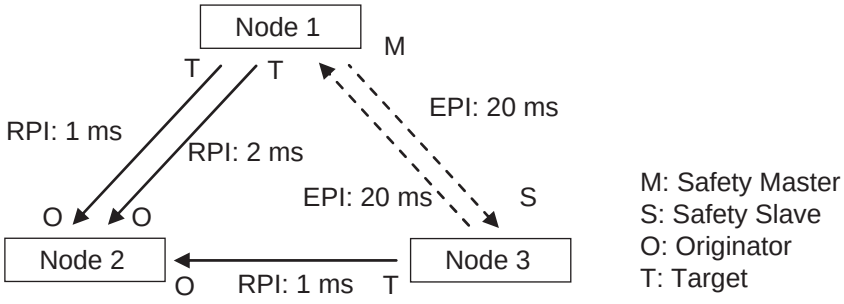
- EPI of 20 ms for connections to send and an EPI of 20 ms for connections to receive at the Safety Master, and
- RPI of 1 ms to send and RPI of 2 ms to receive for Target connections.

Node 2 has:

- RPI of 2 ms to send and RPI of 1 ms to receive for Originator connections.

Node 3 has:

- EPI of 20 ms for connections to send and EPI of 20 ms for connections to receive at the Safety Slave, and
- RPI of 1 ms to send at the Target connection.



The total PPS for each node is calculated as follows:

- Total PPS for EIP Unit of Node 1
  = 1000/20 ms + 1000/20 ms + 1000/1 ms + 1000/2 ms
  = 50 + 50 + 1000 + 500 = 1600 pps
- Total PPS for Unit of Node 2
  = 1000/2 ms + 1000/1 ms + 1000/1 ms
  = 500 +1000 + 1000 = 2500 pps
- Total PPS for Unit of Node 3
  = 1000/20 ms + 1000/20 ms + 1000/1 ms
  = 50 + 50 + 1000 = 1,100 pps

Data can be sent and received for any of the above because the allowed Unit communications bandwidth is 6,000 pps max.

Ethernet Switching Hub Functions

The switching hub functions shown in the following table determine the communications performance of EtherNet/IP.

Item	Description
Buffer capacity	This is the amount of data that can be buffered when packets accumulate at the switching hub.
Multicast filter function	This function transfers multicast packets to the specific nodes only.
QoS function	This function performs priority control on packet transfers.

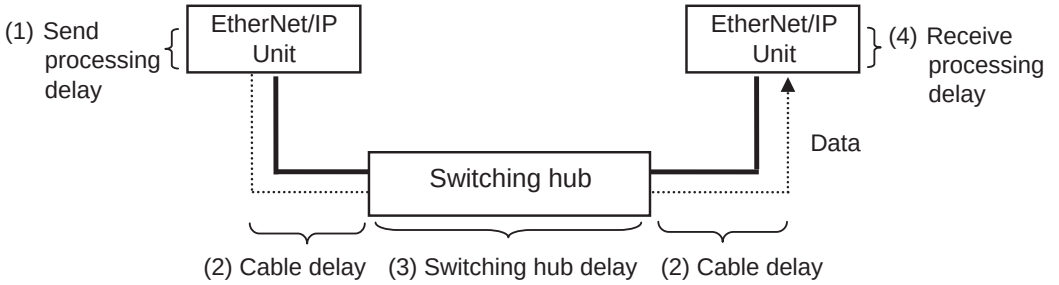
When the settings for Safety I/O Communications and Tag Data Links exceed the capabilities of the switching hub being used, increase the values for the EPI and RPI and make the settings again.

In addition, if the required Tag Data Link performance cannot be achieved with the switching hub's capabilities, reevaluate the overall network configuration and correct it by taking steps such as selecting a different switching hub or splitting the network.

Delay Time in Tag Data Links

In an EtherNet/IP network, the Tag Data Link packets are sent once each packet interval (RPI), but several delays occur between the transmission of packets from each node and the arrival of the packets at the destination nodes. The following diagram shows the 4 major delay sources.

Total network delay = (1) Send processing delay + (2) Cable delays
+ (3) Switching hub delay
+ (4) Receive processing delay



The lengths of these delays depend on many factors, such as the Tag Data Link connection settings (number of connections and data sizes), number of nodes, the switching hub being used, and cable lengths. Each delay is described in detail below.

Send Processing Delay

The send processing delay is the delay that occurs within the EtherNet/IP Unit when data packets are sent once each packet interval. This delay varies with the RPI error shown in the following graph, so the send processing time is the maximum value for each RPI.

Packet interval (RPI)	RPI error (%) (update accuracy cycle)
1 to 500 ms	RPI ±15%
501 ms to 1 s	RPI ±10%
1.001 s to 10 s	RPI ±5%

Cable Delay

The cable delay is the time required for the data signal to pass through the cable and reach the destination. When category 5 or 5e STP (shielded twisted-pair) cable is being used, the maximum cable delay is 545 ns/100 m. The cable delay represents a very small percentage of the total Tag Data Link delay.

Switching Hub Delay

The switching hub delay is the delay time between the arrival of the packet at the switching hub and the output of the packet from the hub's transmission port. This delay depends on the total number of connections used for reception and data sizes used in the Tag Data Links. In addition, this delay depends on the switching hub manufacturer and model. For OMRON W4S1-series Switching Hubs, the delay can be approximated with the following table. For information on the delays for hubs made by other manufacturers, contact the switching hub manufacturer.

The following values are the delays when cascade connections are not being used. If cascade connections are used, more nodes can be connected, but the switching hub delays will increase.

Number of connections used for reception Data size per connection (bytes)	16	32	64	128	256
32 byte	0.2	0.3	0.6	1.2	2.4
128 byte	0.3	0.5	1.1	2.2	4.4
256 byte	0.4	0.9	1.8	3.5	7.0
512 byte	0.8	1.5	3.1	6.1	12.2
1024 byte	1.4	2.8	5.7	11.4	22.7

Unit: ms

Receive Processing Delay

The receive processing delay is the delay that occurs within the EtherNet/IP Unit from the reception of the data packet at the Unit until the completion of reception processing in the Unit. This delay depends on the size of the connections used in the Tag Data Links and the number of connections. In practice, the delay depends on the number of connections used in Tag Data Links with less than 400 bytes. If the number of connections is “n”, the maximum delay can be calculated with the following equation.

Maximum reception processing delay = 1 + (n × 0.043) ms

The size of the connections may cause a delay when the data sizes are smaller and a large number of packets may be received in a fixed interval, because the data may wait for receive processing.

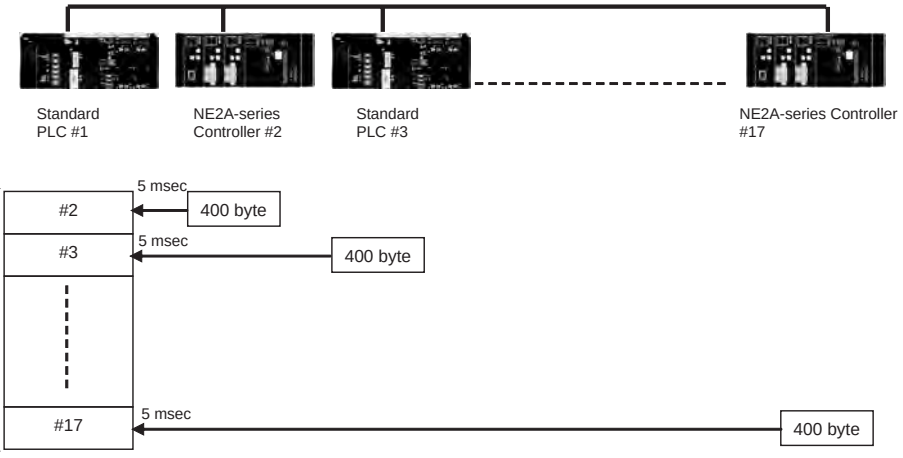
Example Calculation of the Tag Data Link Delay

This example shows how to calculate the Tag Data Link delay when the following Tag Data Link connection settings have been made.

In this case, 17 EtherNet/IP Units are being used, and one Unit is receiving 256 bytes of data from each of the other Units at a packet interval (RPI) of 5 ms. Thus, 16 Tag Data Link connections are used. The length of the cables between the Units is 50 m for all connections.

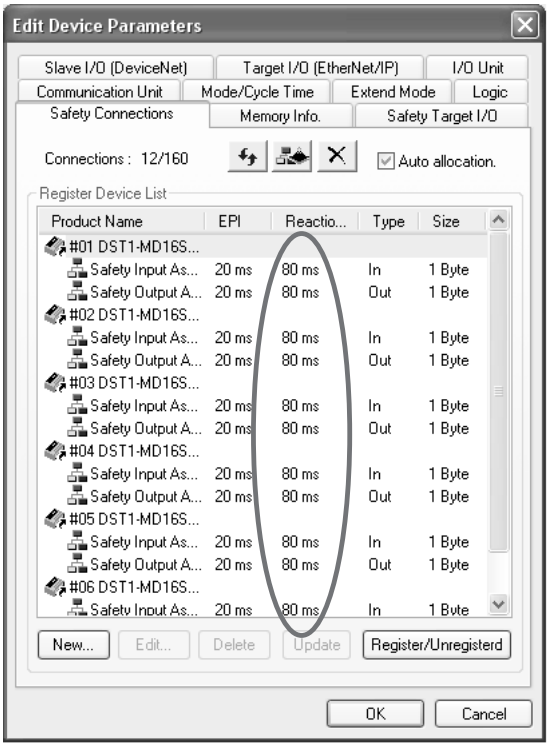
Send processing delay = 15% of 5 ms = 0.75 ms
Cable delay = 545 ns × 50/100 = 272.5 ns
Switching hub delay = 0.4 ms
Receive processing delay = 1 + (16 × 0.043) = 1.688 ms

Tag Data Link delay= 0.75 ms + 0.000272.5 ms + 0.4 ms + 1.688 ms
≅ 2.84 ms



8-5-3 Checking the Network Reaction Time

The network reaction time can be calculated when the EPI is set in the Network Configurator. Refer to the reaction time for each safety connection to see how the network reaction time will function depending on the EPI settings for each safety connection.


Edit Device Parameters
Slave I/O (DeviceNet)
Target I/O (EtherNet/IP)
I/O Unit
Communication Unit
Mode/Cycle Time
Extend Mode
Logic
Safety Connections
Memory Info.
Safety Target I/O
Connections : 12/160
Auto allocation.
Register Device List
Product Name
EPI
Reactio...
Type
Size
#01 DST1-MD16S...
Safety Input As... 20 ms 80 ms In 1 Byte
Safety Output A... 20 ms 80 ms Out 1 Byte
#02 DST1-MD16S...
Safety Input As... 20 ms 80 ms In 1 Byte
Safety Output A... 20 ms 80 ms Out 1 Byte
#03 DST1-MD16S...
Safety Input As... 20 ms 80 ms In 1 Byte
Safety Output A... 20 ms 80 ms Out 1 Byte
#04 DST1-MD16S...
Safety Input As... 20 ms 80 ms In 1 Byte
Safety Output A... 20 ms 80 ms Out 1 Byte
#05 DST1-MD16S...
Safety Input As... 20 ms 80 ms In 1 Byte
Safety Output A... 20 ms 80 ms Out 1 Byte
#06 DST1-MD16S...
Safety Input As... 20 ms 80 ms In 1 Byte
New...
Edit...
Delete
Update
Register/Unregisterd
OK
Cancel

8-6 Checking and Adjusting the System Response Performance

Check that the reaction time satisfies the necessary specifications for the safety chain based on the information in *8-2 Calculating Safety Response Performance*. Check that the standard response performance satisfies the necessary specifications given in *8-3 Calculating Response Performance in Standard Communications.* Make adjustments as described below if the reaction time does not satisfy the necessary specifications.

Adjusting the Network Bandwidth, EPI, and Communications Cycle for Safety Communications and Standard Communications

If Safety I/O Communications and Standard I/O Communications or Tag Data Links are both used, calculate the reaction time for each type of communications while changing the network bandwidth usage.

- To decrease the EPI for Safety I/O Communications and increase the communications cycle time or Tag Data Link RPI for Standard I/O Communications, increase the bandwidth proportion for safety communications.
- Conversely, to decrease the communications cycle time or Tag Data Link RPI for Standard I/O Communications and increase the EPI for Safety I/O Communications, increase the proportion for Standard I/O Communications or Tag Data Link Communications.

Reevaluate the network configuration considering the points in the following sections if any of following conditions occurs even when the calculation that is described above is performed:

- It is not possible to calculate the best average EPI for the desired connection and the best communications cycle time or RPI for the Standard Master.
- The peripheral servicing cycle time of the NE2A-series Controller is longer than the best average EPI.

Dividing Networks

- Divide the DeviceNet network into a Safety Network and Standard Network if Safety I/O Communications and Standard I/O Communications are both used.
- Divide the network into two DeviceNet Safety Networks if only Safety I/O Communications are used.
- Divide the EtherNet/IP network into a Safety Network and Standard Network if both Safety I/O Communications and Tag Data Link Communications are used.

Adding Controllers to Perform Distributed Control

Change the Slave from a DST1-series Controller to a NE0A-series Controller to enable distributed control if high-speed reaction time is required for some I/O.

SECTION 9
Basic Network Configurator Operations

This section describes how to use the Network Configurator with a NE2A-series Safety Network Controller.

9-1 Checking before Installation 194
9-1-1 System Requirements 194
9-1-2 Required Software Installations 194
9-2 Installing the Network Configurator 195
9-2-1 Installing the Network Configurator 195
9-2-2 Uninstalling the Network Configurator 196
9-3 Installing the USB Driver 198
9-3-1 Installing the USB Driver 198
9-4 Starting and Exiting the Network Configurator 207
9-4-1 Starting and Exiting the Network Configurator 207
9-4-2 Checking the Version 208
9-5 Saving and Reading Network Configuration Files 210
9-5-1 Saving Network Configuration Files 210
9-5-2 Reading Network Configuration Files 212
9-5-3 Password Protection for Network Configuration Files 214
9-5-4 Protection Mode 216
9-5-5 Reading Network Configuration Files Created with Network Configurator Version 2.□ or Lower 217
9-6 Main Window and Menus 218
9-6-1 Main Window 218
9-6-2 Network Configuration Pane 218
9-6-3 Network Configuration List 221
9-6-4 Menu Commands 222
9-6-5 Status Bar 228

9-1 Checking before Installation

Before installing the Network Configurator, check items such as system requirements.

9-1-1 System Requirements

To install the Network Configurator, the following system requirements must be satisfied. The applicable operating systems depend on the version of the Network Configurator.

Item	System requirements
Operating system (OS), Japanese or English	Windows XP (Service Pack 3 or higher except for 64-bit version) Windows Vista (Service Pack 2 or higher) Windows 7
Computer	A computer with a processor recommended by Microsoft Corporation.
Memory	The memory capacity recommended by Microsoft Corporation.
Hard disk	At least 200 MB of available space is required.
Display	SVGA (800 × 600 pixels) or better high-resolution display with at least 256 colors
Disk drives	CD-ROM drive
Mouse	A mouse or other pointing devices that is compatible with Windows is required.
Communications ports (See note)	At least one of the following communications ports is required. • USB port: To go online via a USB port (USB 1.1) on the NE2A-SCPU. • Ethernet port: To go online via Ethernet. • DeviceNet Interface Card (3G8F7-DRM21 or 3G8E2-DRM21-V1): To go online via DeviceNet.

Note (1) The computer cannot be placed on standby while it is connected to an NE2A-series Controller with a USB cable.

(2) The DeviceNet Interface Card is not compatible with a 64-bit OS.

9-1-2 Required Software Installations

The Network Configurator must be installed. In addition, communications software must be installed to connect to the NE2A-series System.

- USB driver: To connect online via USB
- DeviceNet Interface Card driver: To connect online using a DeviceNet Interface Card

Installing the Network Configurator

Refer to *9-2 Installing the Network Configurator*.

Installing the USB Driver

Refer to *9-3 Installing the USB Driver*.

Installing the DeviceNet Interface Card Driver

Refer to the manual for the 3G8F7-DRM21 or 3G8E2-DRM21-V1 DeviceNet Interface Card and install the DeviceNet Interface Card driver.

9-2 Installing the Network Configurator

This section describes how to install and uninstall the Network Configurator.

9-2-1 Installing the Network Configurator

Preparing for Installation

Check the following items before beginning with the installation.

■ **Available Hard Disk Space**

The Network Configurator can be installed on the hard disk only. At least 200 MB of hard disk space is required. Make sure that there is enough space available.

■ **Windows Environment and Installation Folder**

The Network Configurator is a software application for a Windows operating environment. The software is installed on top of Windows. Make sure that Windows is installed and functioning correctly on the computer. Also, make sure that you are logged onto the computer as a user with administrator rights.

Note With version 3.3□ or higher, if Network Configurator version 3 has already been installed from a different package, such as the CX-One, then the previous installation is updated.

Installation Precautions

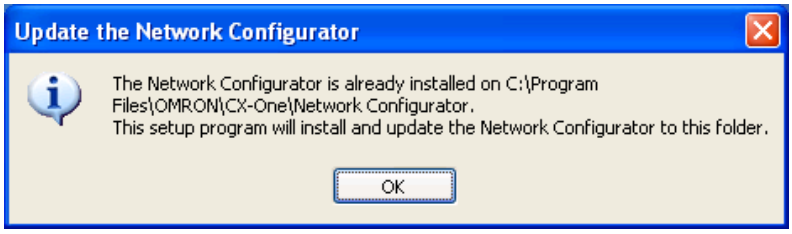
- If Network Configurator version 3 has already been installed from a different package, such as the CX-One, then the previous installation is updated. Files will be installed in the same folder as the one used by the previous package to upgrade functionality.
- If you install the software again from the CX-One after installing the Network Configurator, installation of Network Configurator for EtherNet/IP will overwrite some of the files. As a result, some problems will occur, e.g., some devices will not be displayed in the Hardware List Pane.
  These problems can be solved by applying a patch.
  Execute the \Utility\CX-One_Update\Ntc****_****Setup_for_Safety.exe files (where * indicates any number) in the Network Configurator Master Disk and install the patch according the instructions from the installer.

Installation Procedure

1,2,3...

1. Insert the Network Configurator Master Disk into the CD-ROM drive. Open the CD-ROM drive from the Explorer and execute the setup.exe file.
2. Complete the installation process following the instructions provided on-screen.

Note You can specify the folder in which to install the Network Configurator during the installation process. However, if the same version of the Network Configurator has already been installed from a different package, such as the CX-One, the installation folder cannot be changed (because an update installation will be performed).



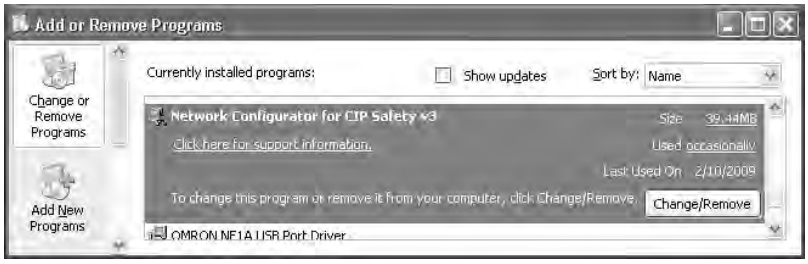
9-2-2 Uninstalling the Network Configurator

This section describes the procedure for installing the Network Configurator.

Procedure

1,2,3...

1. Select ***Control Panel*** from the Windows Start Menu.
2. For Windows Vista or Windows 7, select ***Programs and Features***.
   For Windows XP, select ***Add or Remove Programs***.
   For Windows 2000, select ***Add/Remove Programs***.
   A dialog box will be displayed. The dialog box will depends on the operating system.
   The Add or Remove Program Dialog Box is shown below as an example.

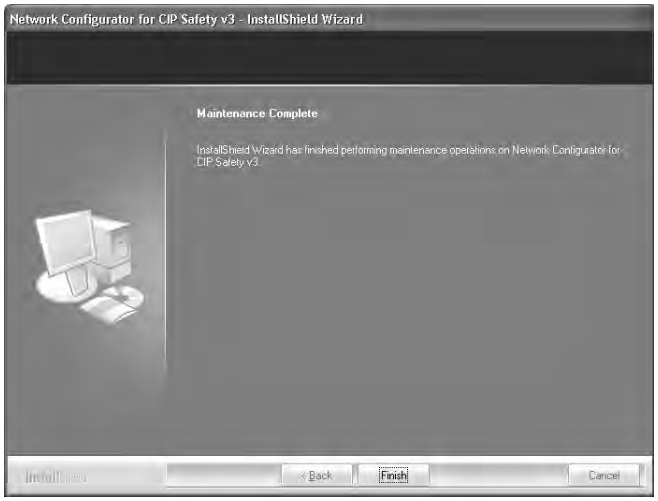


3. Select *Network Configurator for CIP Safety v3* and click the **Change/Remove** Button. (For Windows Vista or Windows 7, click the **Uninstall** Button.)
   A dialog box will be displayed to confirm the deletion.



4. Click the **Yes** Button.
   (If you click the No Button, the uninstallation will not be completed, and the InstallShield Wizard Complete Dialog Box will be displayed.)
   A dialog box that shows the setup status will be displayed, and the uninstallation will start.

   If the uninstallation is completed successfully, the InstallShield Wizard Complete Dialog Box will be displayed.



5. Click the **Finish** Button.

9-3 Installing the USB Driver

9-3-1 Installing the USB Driver

You must install the USB driver to go online with the NE1A-series, NE0A-series, or NE2A-series Controller via USB.

Preparing for Installation

Check the following items before beginning with the installation.

■ **Connection to a Safety Network Controller**

Turn ON the power supply to the Safety Network Controller (NE1A, NE0A, or NE2A) and then use a USB cable to connect the USB port on the Safety Network Controller to the USB port on a computer on which the Network Configurator has already been installed.

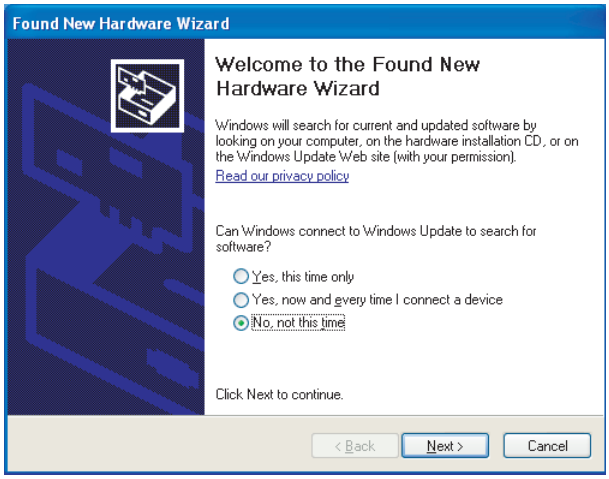
■ **Windows Environment**

Make sure that you are logged onto the computer as a user with administrator rights.

Installing on Windows XP

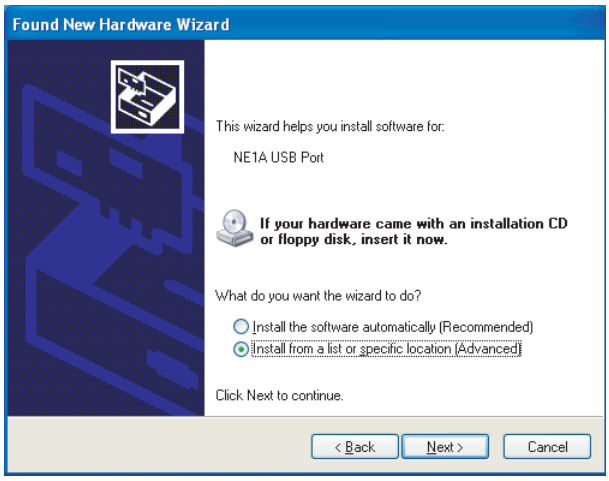
Operating Procedure

1,2,3... 1. The computer will automatically detect the Safety Network Controller when the cable is connected and display a message saying that new hardware has been detected. The Found New Hardware Wizard will be displayed.

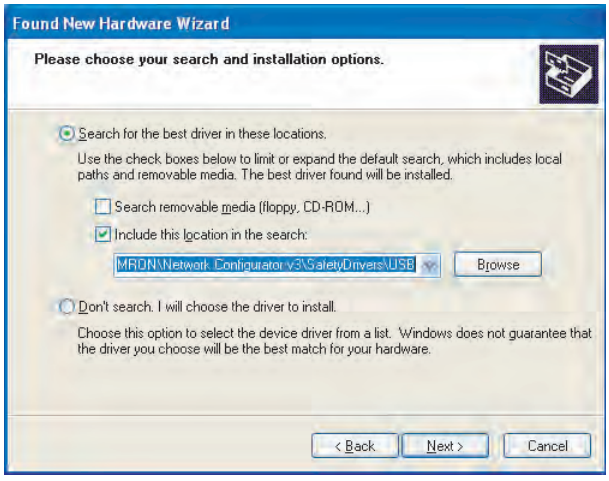


In the Found New Hardware Wizard Dialog Box, select the *No, not this time* option and click the **Next** Button.

2. Select the *Install from a list or specific location (Advanced)* Option and click the **Next** Button.



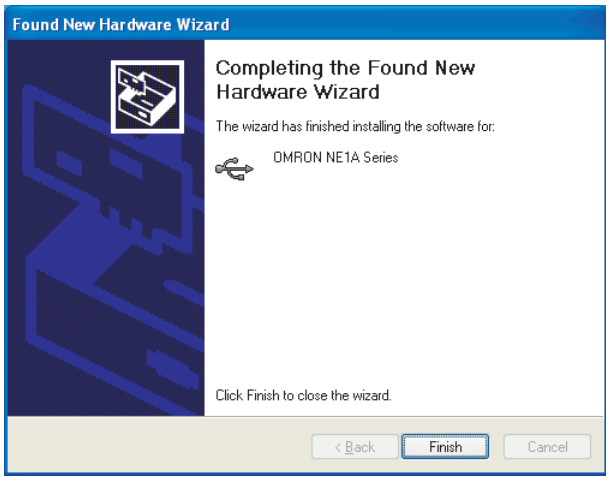
3. Select the *Search the best driver in these locations* Check Box and select the *Include this location in the search* Option. Click the **Browse** Button, select the \SafetyDrivers\USB folder in the folder in which the Network Configurator was installed or the \drivers\USB folder in the Network Configurator Master Disk (CD-ROM), and the click the **Next** Button.



4. If a warning message appears saying that the driver has not passed the Windows logo test, ignore it and click the **Continue Anyway** Button.



5. When the driver installation is completed normally, the following dialog box will be displayed. Click the **Finish** Button.



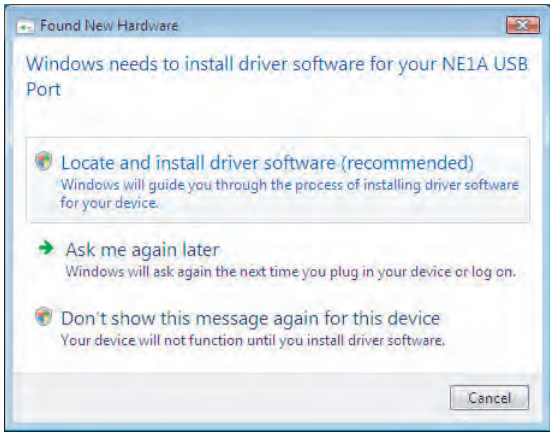
6. If you are using an NE1A-series or NE0A-series Controller, two different drivers must be installed. The Found New Hardware Wizard Dialog Box will be displayed again. Perform the installation using the procedure in step 1-5.

Note If an NE1A-series, NE0A-series, or NE2A-series Controller is connected to a computer on which the driver has been installed only once, the Found New Hardware Wizard Dialog Box will be displayed again. If it is displayed, select the *Search for a suitable driver for my device (recommended)* Option and then continue with the procedure.

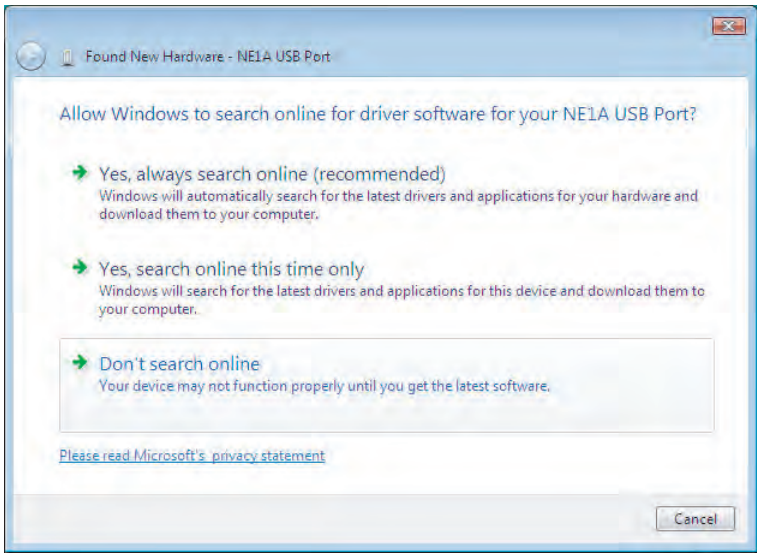
Installing on Windows Vista

Operating Procedure

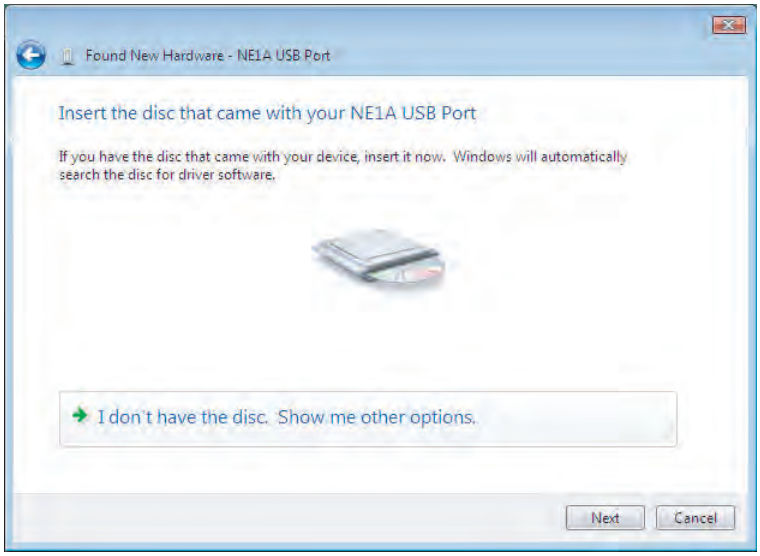
1,2,3... 1. When the computer detects the Safety Network Controller, the Found New Hardware Dialog Box will be displayed. Select the *Locate and install driver software (recommended)* Option.



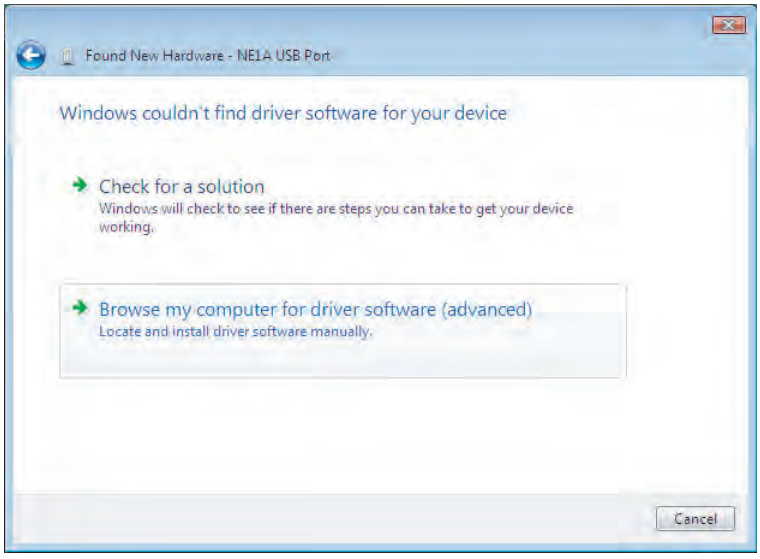
2. If the following dialog box is displayed, select the *Don't search online* Option.



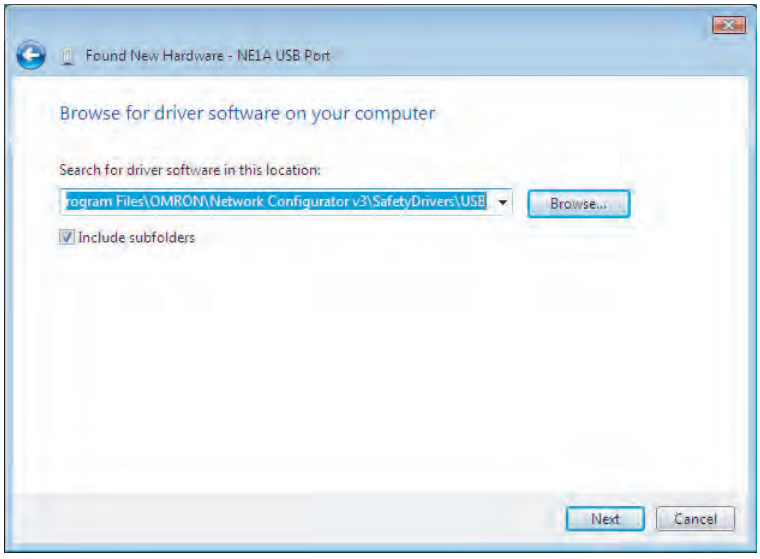
3. Select the following: *I don't have the disc. Show me other options*.



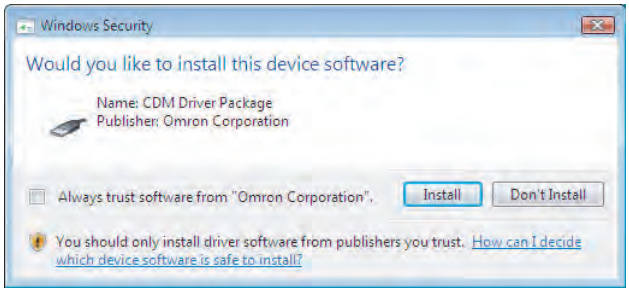
4. Select the *Browse my computer for driver software (advanced)* Option.



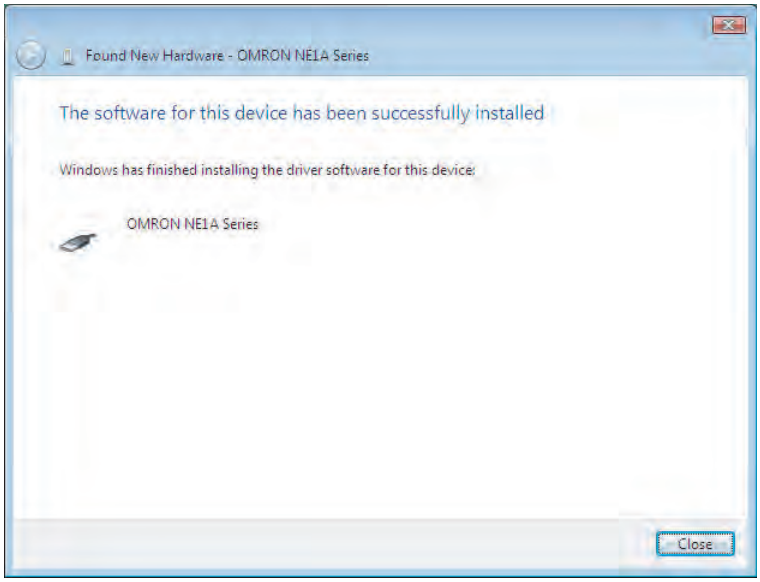
5. Under *Search for driver software in this location*, click the **Browse** Button, select the \SafetyDrivers\USB folder in the folder in which the Network Configurator was installed or the \drivers\USB folder in the Network Configurator Master Disk (CD-ROM), and the click the **Next** Button.



6. The Windows Security Dialog Box will be displayed. Click the **Install** Button.



7. When the driver installation is completed normally, the following dialog box will be displayed. Click the **Close** Button.

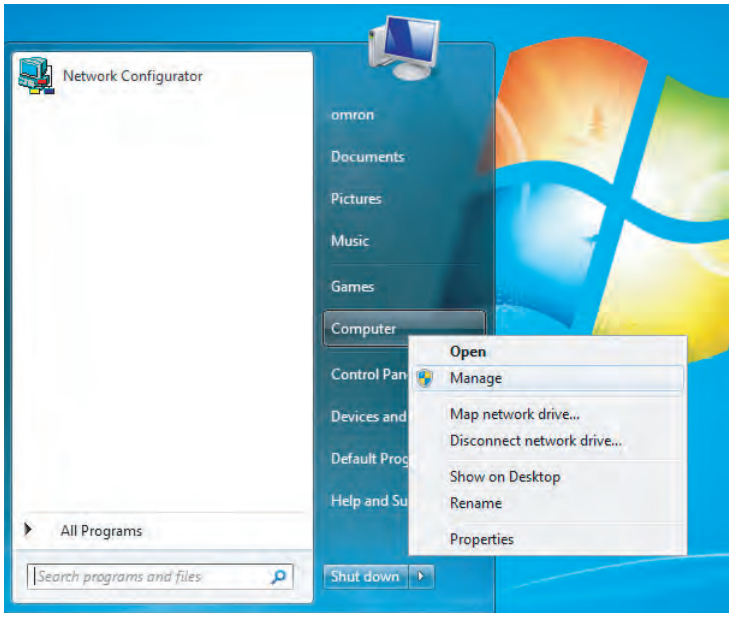


8. If you are using an NE1A-series or NE0A-series Controller, two different drivers must be installed. The Found New Hardware Dialog Box will be displayed again. Perform the installation using the procedure in step 1-7.

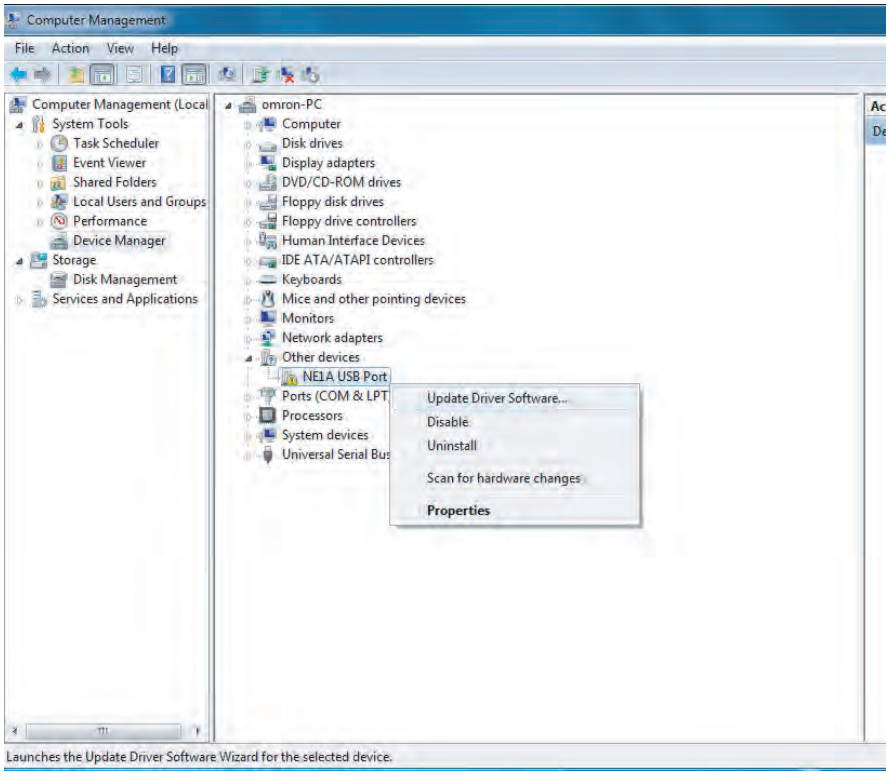
Installing on Windows 7

Operating Procedure

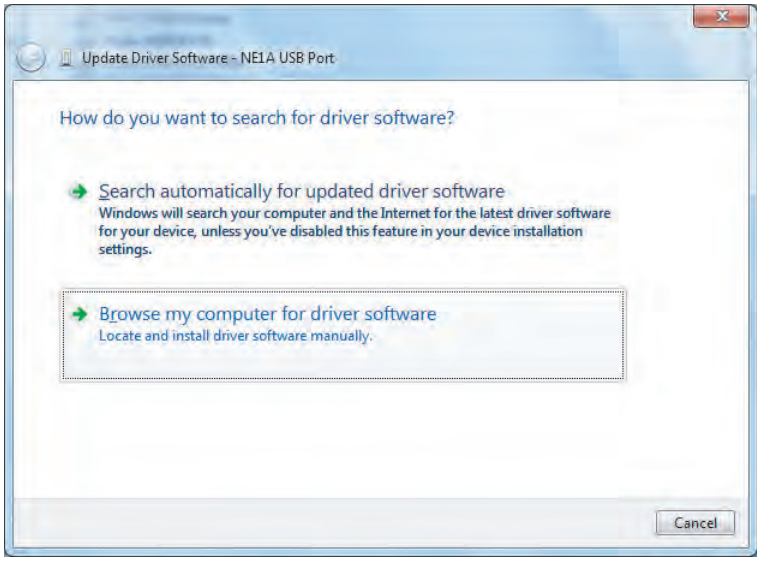
1,2,3... 1. Right-click ***Computer*** on the Start Menu, and then select ***Manage***.



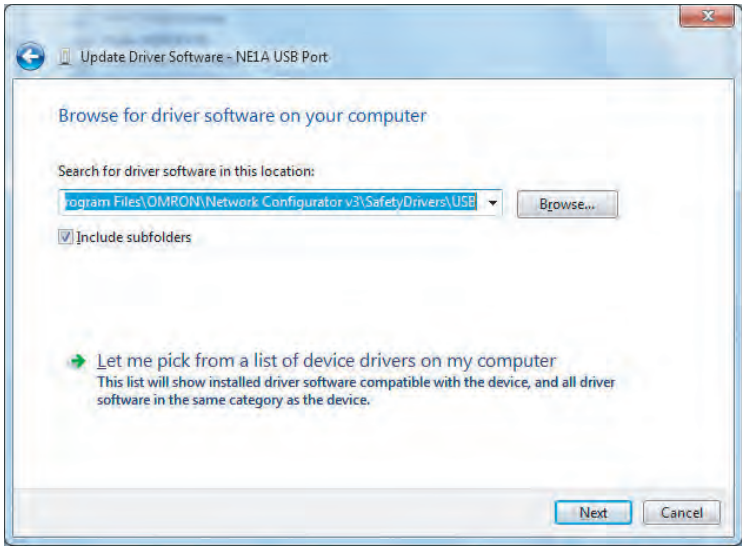
2. Select the Device Manager on the navigation pane. Right-click ***NE1A USB Port, NE0A USB Port, or OMRON-PLC*** under *Other Devices*, and then select ***Update Driver Software***.



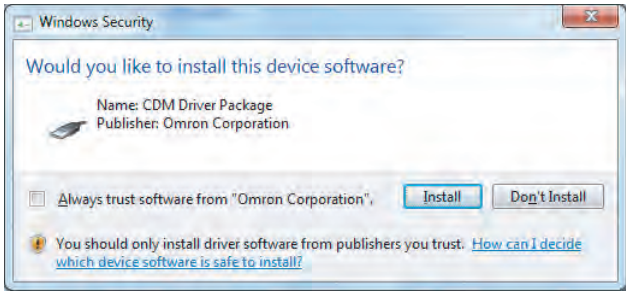
3. The Update Driver Software Dialog Box will be displayed. Select the *Browse my computer for driver software* Option.



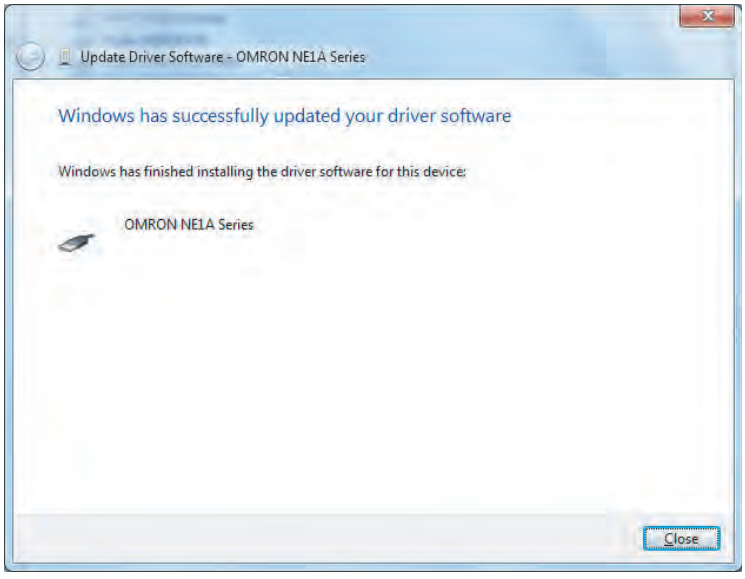
4. Under *Search for driver software in this location*, click the **Browse** Button, select the \SafetyDrivers\USB folder in the folder in which the Network Configurator was installed or the \drivers\USB folder in the Network Configurator Master Disk (CD-ROM), and the click the **Next** Button.



5. The Windows Security Dialog Box will be displayed. Click the **Install** Button.



6. When the driver installation is completed normally, the following dialog box will be displayed. Click the **Close** Button.



7. If you are using and NE1A-series or NE0A-series Controller, repeat step 1-2. *USB Serial Port* will be displayed under *Other Devices*. Perform the installation using the procedure in step 2-6.

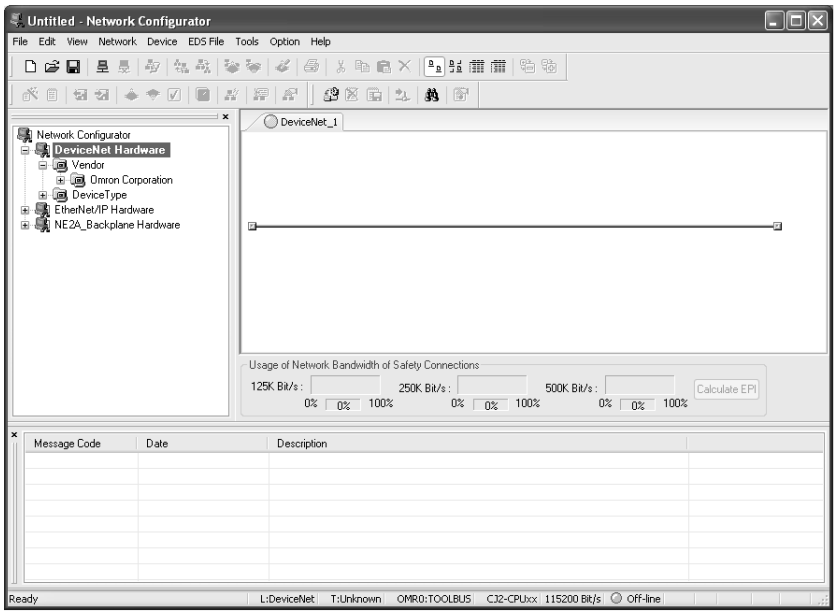
9-4 Starting and Exiting the Network Configurator

This section describes how to start and exit the Network Configurator, and how to check the version.

9-4-1 Starting and Exiting the Network Configurator

Starting the Network Configurator

Select ***(All) Programs - OMRON Network Configurator for CIP Safety v3*** from the Windows Start Menu. The Network Configurator will be started and the Main Window will be displayed.



■ **Starting as Administrator**

To perform the following procedures, start the Network Configurator as the system administrator.

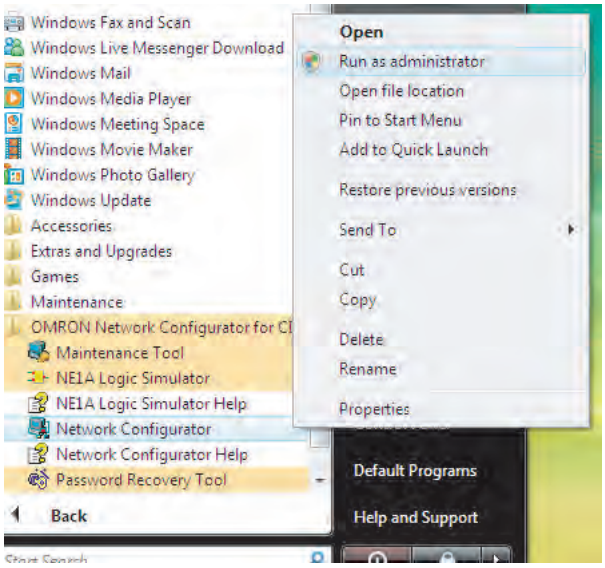
- Installing, creating, or deleting EDS files or creating EDS index files
- Editing settings files, installing plug-in modules, installing interface modules
- Saving, deleting, or importing user-defined function blocks
- Registering or deleting folders in the libraries
- Registering user-defined function blocks or sections in libraries

Windows 2000 or Windows XP

1. Log onto Windows as a user with administrator rights.
2. Select ***All Programs - OMRON Network Configurator for CIP Safety v3 - Network Configurator*** from the Windows Start Menu.

Windows Vista or Windows 7

1. Right-click ***All Programs - OMRON Network Configurator for CIP Safety v3 - Network Configurator*** in the Windows Start Menu.
2. Select Run as administrator from the pop-up menu that is displayed.



Exiting the Network Configurator

Select ***Exit*** from the File Menu. The Network Configurator will be closed.

9-4-2 Checking the Version

Use the following procedure to check the Network Configurator version.

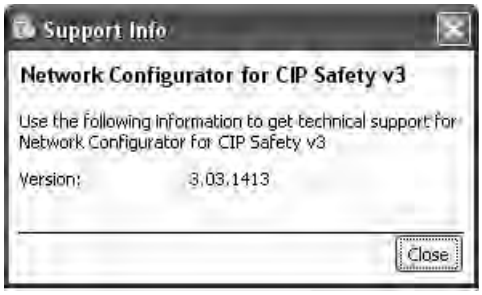
Procedure

1,2,3...

1. Select ***Control Panel*** from the Windows Start Menu.
2. For Windows Vista, select ***Programs*** from the Control Panel.
   For Windows XP, select ***Add or Remove Programs*** from the Control Panel.
   For Windows 2000, select ***Add/Remove Programs*** from the Control Panel.
   The Add or Remove Programs Dialog Box will be displayed.
3. Select *Network Configurator for DeviceNet Safety v3* from the list of currently installed programs.



4. Click the *Click here for support information* Link. (For Windows Vista, click the **View** Button. The Support Info Dialog Box will be displayed.



5. Check the version and click the **Close** Button.

9-5 Saving and Reading Network Configuration Files

This section describes network configuration file management procedures.

Network configurations created with the Network Configurator can be saved to files and read from the files.
Files can be saved and read in any of the following units: normal (all), network, or device. In addition, network configuration files can be protected by passwords.

9-5-1 Saving Network Configuration Files

This section describes how to save all files (normal) or to save files by network or device.

Normal (Saving All)

The entire system can be saved as a batch. When opening the files, it is also possible to specify the network.

Procedure

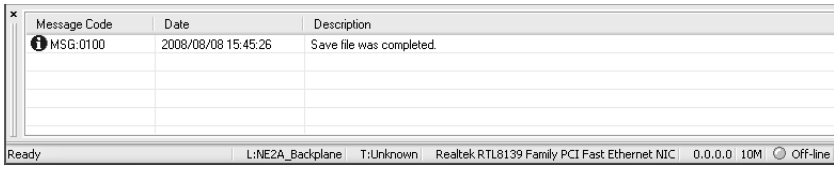
1,2,3...

1. Select ***Save*** or ***Save As*** from the File Menu, or click the **Save Network Configuration** Button in the toolbar. The standard Windows dialog box for saving will be displayed.
2. Specify the save location and the file name, and click the Save Button. If the file is being saved for the first time, the Set Password Dialog Box will be displayed.
   From the second time onwards, the Confirm Password Dialog Box will be displayed.
   For details, refer to *9-5-3 Password Protection for Network Configuration Files*.

Note

- For security, it is recommended that passwords be set for network configuration files.
- Once a password has been set, do not forget it. If the password is forgotten, that network configuration file cannot be edited.

3. In the Set Password Dialog Box, input the password to be set for the network configuration file.
   In the Confirm Password Dialog Box, input the password that was set when the network configuration file was saved.
   When the file has been successfully saved, it will be displayed in the Message Report Pane as shown below.



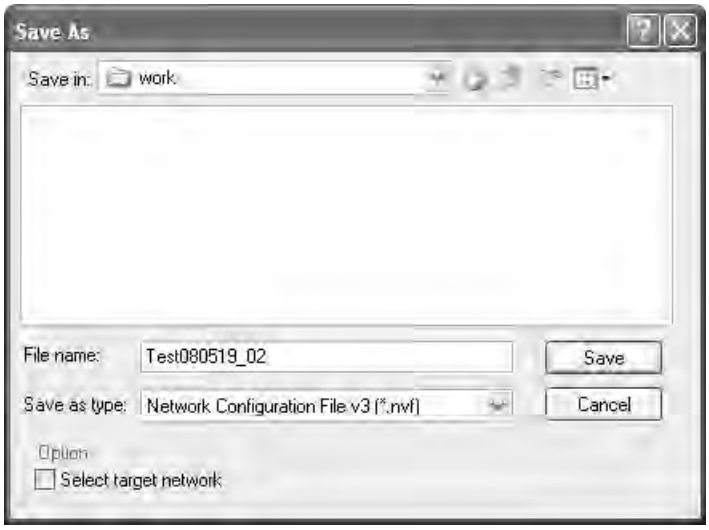
Saving Network Configuration Files by Network

Network configurations can be reused. It is possible to save the network configuration file by network and specify the network when opening the file.

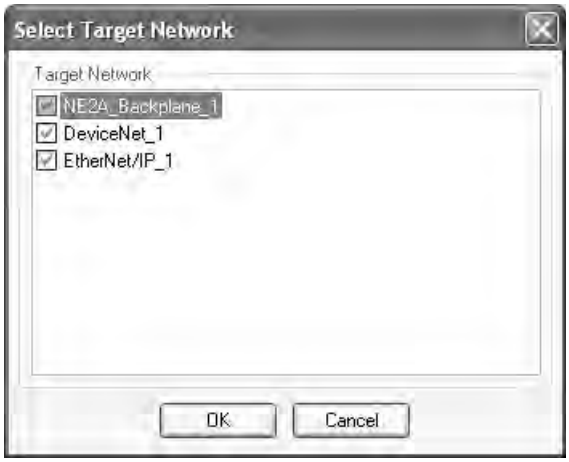
Procedure

1,2,3...

1. Select ***Save As*** from the File Menu.
   The Save As Dialog Box will be displayed.



2. All network data will be saved if you click the Save Button without selecting the *Select Target network Option*. Select the *Select Target network Option* and click the **Save** Button.
   The Confirm Password Dialog Box will be displayed.
3. Enter a password and click the **OK** Button.
   The Select Target Network Dialog Box will be displayed.



4. Select the network you want to save in the Select Target Network Dialog Box. (Clear the selections for the networks that you do not want to save.)
5. Click the **OK** Button. The data of the selected network will be saved to a file.

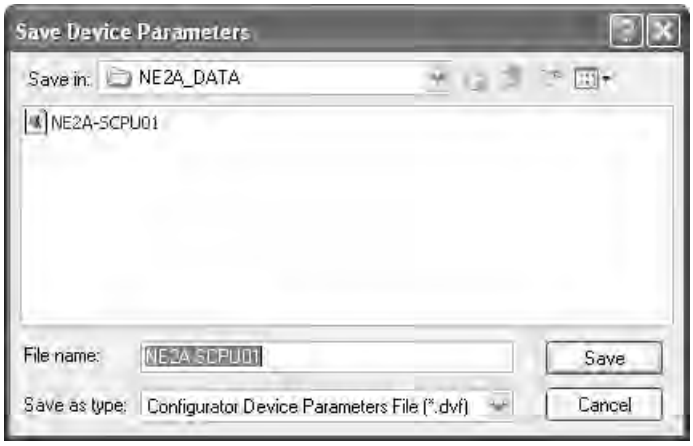
Saving Network Configuration Files by Device

Network configurations can be reused by device.

Procedure

1,2,3...

1. Select the device and select ***Parameter - Save*** from the Device Menu.
   You can also press the shortcut key and select ***Parameter - Save*** from the menus.
   The Save Device Parameters Dialog Box will be displayed.



2. Select the location for saving the file, enter a name, and click the Save Button. The device configuration data will be saved.

9-5-2 Reading Network Configuration Files

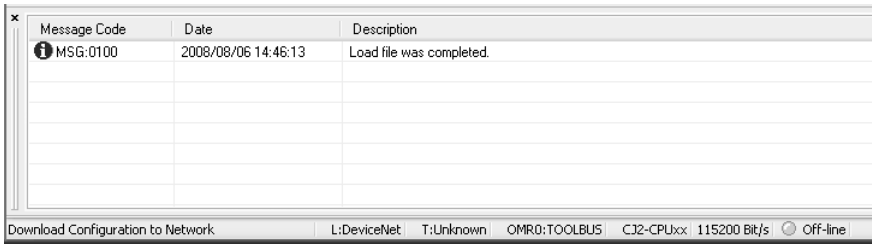
It is possible open the saved network configuration file for individual networks and to make additions to existing network configurations for individual networks.

Normal Reading

Procedure

1,2,3...

1. Select ***Open*** from the File Menu. You can also click the **Open Network Configuration** Button in the toolbar.
   The standard Open File Dialog Box in Windows will be displayed.
2. Select the file and click the **Open** Button.
   The confirm password dialog box will be displayed.
3. Enter the password that you set when you saved the network configuration file.
   If the data reading is completed successfully, a message such as the following will be displayed in the Message Report Pane.

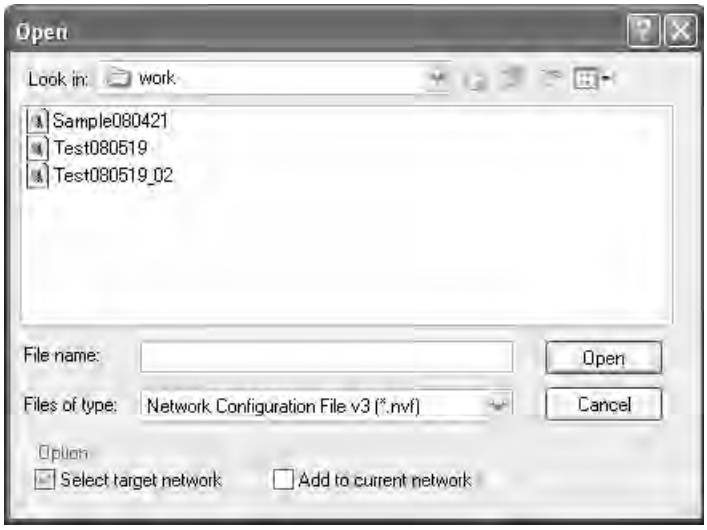


Selecting a Network and Reading the Network Configuration File

Procedure

1,2,3...

1. Select ***Open*** from the File Menu.
   You can also click the **Open Network Configuration** Button in the toolbar.
   The standard Open Dialog Box in Windows will be displayed.



2. Select the *Add to current network* Check Box and click the **Open** Button. The network data read from the file will be added to the network being used.

   Select the *Select Target network* Check Box and click the **Open** Button. Use the following procedure to read the configuration file of the network. The Confirm Password Dialog Box will be displayed.



3. Enter the password and click the **OK** Button.
   The Select Network Dialog Box will be displayed.



4. Select the networks to use. (Clear the selection of any network that you will not use.)
5. Click the **OK** Button.
   The data of the selected networks will be read.

Reading Network Configuration Files by Device

Procedure

1,2,3...

1. Place the same model of device in the virtual network as the device that data will be read from.
2. Select the device and select ***Parameter - Read*** from the Device Menu. You can also press the shortcut key and select ***Parameter - Save*** from the menus.
   The Open Device Parameters Dialog Box will be displayed.



3. Name the file and click the **Open** Button. The configuration data for the device will be read and set for the selected device.

9-5-3 Password Protection for Network Configuration Files

Passwords can be set for network configuration files. The password is encrypted and saved in the file. Setting a password prevents unauthorized changes to a network configuration file. The network configuration file password is requested when any of the following operations is attempted with the Network Configurator.

- Saving a network configuration file
- Reading a network configuration file
- Changing the network configuration file password

Password When Saving a File

The Assign Password Dialog Box will always be displayed to prompt the setting of a password if ***Save*** is selected from the File Menu for a file without a password setting or if **Save As** is selected from the File Menu.



Note

- The password can contain from 6 to 16 alphanumeric characters.
- To save the file without setting a password, enter nothing and click the **OK** Button.
- For security, it is recommended that passwords be set for network configuration files.

When a file for which a password has been set is saved, the Confirm Password Dialog Box is displayed.



If the password that is entered does not match the one that was set, an error message will be displayed and the file cannot be saved.

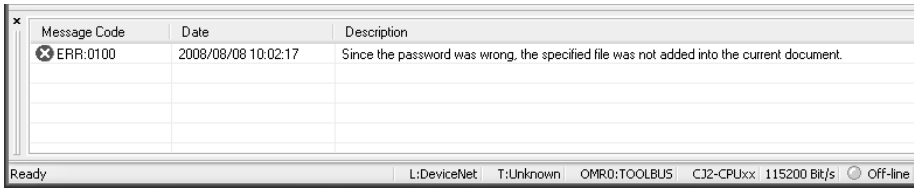
Password When Opening a File

If the password is not correct when opening a file, the file will be opened in Protection Mode.



Some Network Configurator operations are restricted in Protection Mode.
For details on the Protection Mode, refer to *9-5-4 Protection Mode*.

If the password is not correct when making an addition to the current network configuration, an error will occur and the addition will not be allowed.



Changing the Password

A password that has been set for a network configuration file can be changed by selecting ***Change Password*** from the File Menu to display the Change Password Dialog Box.



After the password has been changed, the file must be saved in order to save the new password.

9-5-4 Protection Mode

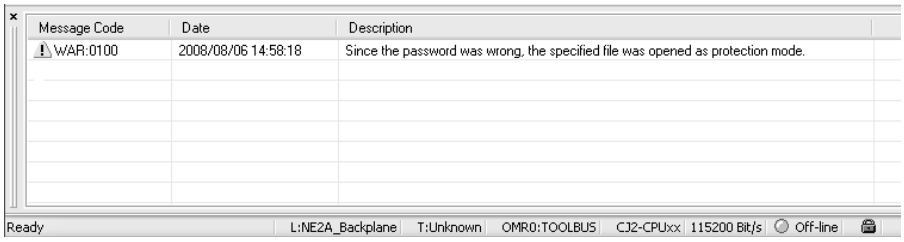
If the password is not correct when opening a network configuration file, the Network Configurator will open the file in Protection Mode.

If the password is incorrect, the following message will be displayed in a message box and in the Message Report Pane.

Message Box



Message Report Pane



The following operations are disabled in Protection Mode.

Menu	Menu command	
File	Save	
	Save As	
	Change Password	
Network	Download	
Device	Parameter	Download
	Reset	
	Change Password	
Tools	Setup Node Address/Baud Rate	

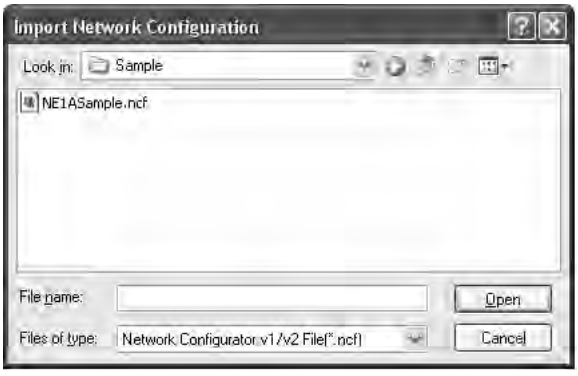
9-5-5 Reading Network Configuration Files Created with Network Configurator Version 2.□ or Lower

Network configuration files created with Network Configurator version 2.□ or lower can be read with Network Configurator version 3.

Procedure

1,2,3...

1. Select ***External Data - Import*** from the File Menu.
   The Import Network Configuration Dialog Box will be displayed.
2. Select the type of file to read in the *Files of type* Box.
3. Select the file to read, and click the **OK** Button.
   The Confirm Password Dialog Box will be displayed.
4. Input the password that was set when the network configuration file was saved.
   The network configuration file will be read.

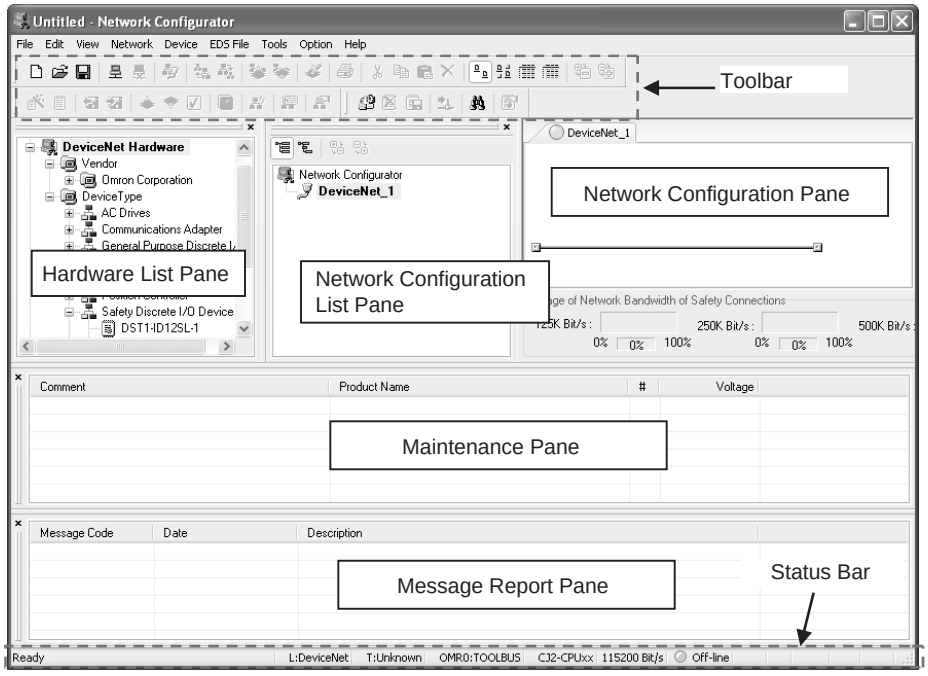


9-6 Main Window and Menus

This section describes the configuration of and menus in the Main Window of the Network Configurator.

9-6-1 Main Window

As shown below, the Main Window basically consists of the Hardware List Pane, the Network Configuration Pane, and the Message Report Pane.



Panes

Pane	Description
Hardware List Pane	Displays the devices that can be added to the network.
Network Configuration Pane	Displays the device configuration registered for the virtual network.
Network Configuration List Pane	Displays the virtual network configuration and path information in a list. (This pane is hidden by default.)
Maintenance Pane	Displays device maintenance information. (This pane is hidden by default.)
Message Report Pane	Displays information such as communications errors.

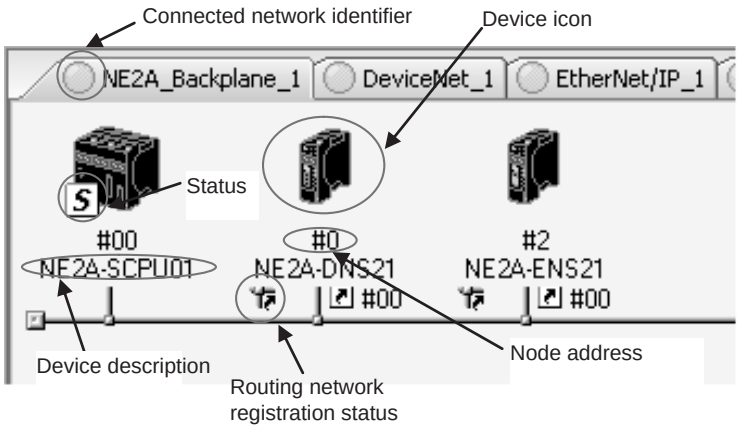
9-6-2 Network Configuration Pane

The display for the Network Configuration Pane can be switched. The following table shows the display modes.

Display mode	Description
Normal Mode	Displays normal mode information.
Maintenance Mode	Displays normal mode information and maintenance information.
Detailed Display 1 Mode (based on Master)	Displays information on devices registered to a Master.
Detailed Display 2 Mode (based on Slaves)	Displays information on devices registered to Slaves.

Normal Mode

The normal mode is the normal display mode. It displays device icons, node addresses, and descriptions of devices.



The following table describes the items.

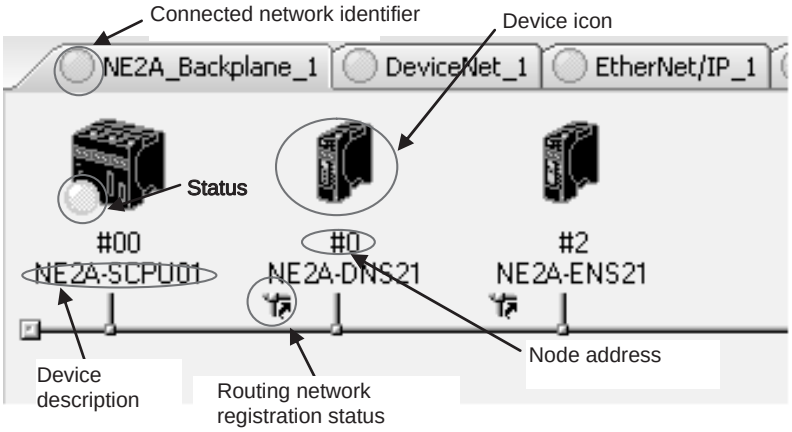
Name	Description
Connected network identifier	These marks identify the networks that are connected online. : The gray icon indicates a network that is offline or not connected online. : The blue icon indicates a network to which the Network Configurator is directly connected online. : The green icon indicates a network that is indirectly connected online via a router device. : The red icon indicates the error status of the network. Refer to *SECTION 19 Troubleshooting* for information on how to handle these errors.
Device icon	Icons are displayed for devices that comprise the network. You can change the icons by selecting *Properties* in the Device Menu.
Device description	This is a character string that describes the device. The default setting is the product name. The product name is displayed when a device is added to a virtual network. You can change the comment by selecting *Change Device Comment* in the Device Menu.
Status	This mark indicates the status of the device. It is displayed only for devices that are safety compliant. The following marks are displayed. : Indicates a safety-compliant device. : Indicates that the device has been verified. **Note** For information on verification, refer to *17-4-1 Verifying Device Parameters*. : Indicates that the device is locked. **Note** For information on unlocking devices, refer to *17-7-2 Locking Configurations*. : Indicates that a locked device was edited.
Node address	Node address of the device
Routing network registration status	This mark indicates the registration status of the routing network. It is displayed only for devices that support routing. : The routing network is not registered. : The routing network is registered.

Note The network tabs that are displayed can be switched by dragging and dropping them.



Maintenance Mode

In addition to providing the information displayed in the normal mode, the maintenance mode enables checking the devices that require maintenance. Device status is also displayed.

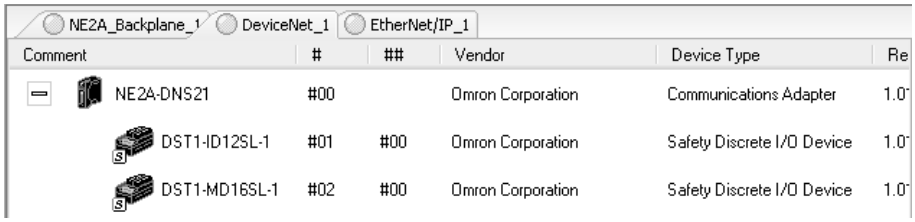


The following table describes the items.

Item	Description
Connected network identifier	Same as for normal mode.
Device icon	Same as for normal mode.
Device description	Same as for normal mode.
Status	This mark indicates the status of the device. It is displayed only for devices that are compliant with DeviceNet Safety. The following marks are displayed. : The gray icon indicates offline status. : The gray icon with the light-blue border indicates default status. **Note** This includes non-configured status. : The green icon indicates IDLE mode. : The blue icon indicates RUN mode (normal). : The yellow icon indicates warning status. : The red icon indicates alarm status.
Node address	Same as for normal mode.
Routing network registration status	Same as for normal mode.

Detailed Display Mode 1 (Based on Master)

The Master device comments, device descriptions, and Master device node address are displayed along with the node addresses, header names, device types, product names, and revisions of the devices registered in the Master. The information on the devices registered in the Master is the information stored in the Master.

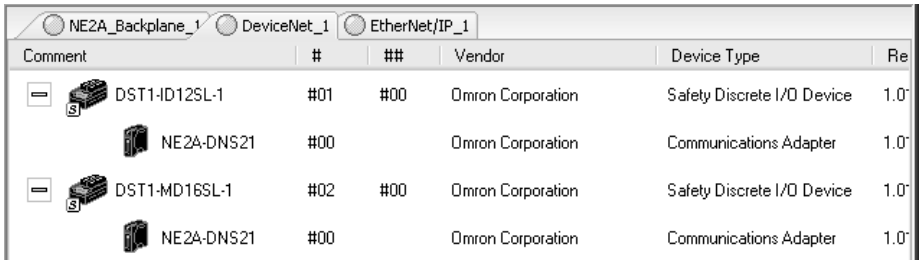


The following table describes the items.

Item	Description
Comment	The comment describes the device. You can change the comment by selecting *Change Device Comment* in the Device Menu.
#	The DeviceNet node address or EtherNet/IP IP address of the device
##	If the device is a Slave, the DeviceNet node address or EtherNet/IP IP address of the Master at registration destination.
Vendor	Name of device vendor
Device Type	Type of device
Rev	Device version
Product Name	Product name of device

Detailed Display 2 (Based on Slaves)

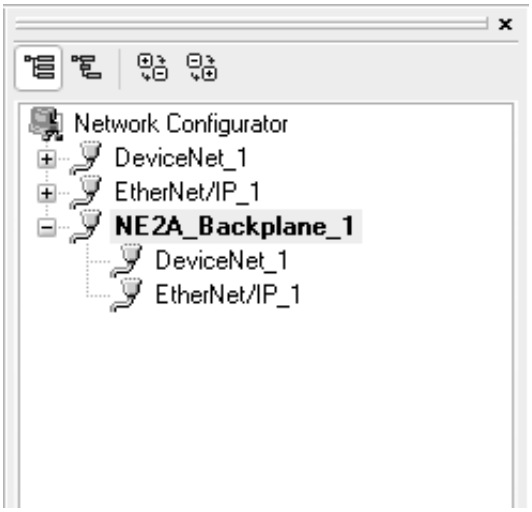
The Master device comments, device descriptions, and Master device node address are displayed along with the node addresses, header names, device types, product names, and revisions of the devices registered in the Master. The information on the devices registered in the Master is the information stored in the Slaves.



For information on these items, refer to *Detailed Display Mode 1 (Based on Master)* on page 220 above.

9-6-3 Network Configuration List

The Network Configuration List Pane displays the configurations of the virtual networks created using the Network Configurator.



You can double-click on a network name to switch the Network Configuration Pane display to the applicable network.

Procedure

Select ***Network Configuration*** from the View Menu.

Toolbar

The following table describes the functions of the toolbar icons at the top of the Network Configuration Pane.

Icon	Description
	Hide Router Devices Displays the router devices in the network configuration list.
	Display Router Devices Displays the router devices in the network configuration list.
	Open All Opens the tree display and displays all of the items.
	Close All Closes the tree display, and displays only the uppermost networks.

9-6-4 Menu Commands

This section describes the function of each menu command of the Network Configurator.
“Online” is the state in which the Network Configurator is connected to the network. “Offline” is the state in which the Network Configurator is disconnected from the network.

File Menu

Menu commands		Description	Toolbar icon	Offline	Online
New	DeviceNet	Creates a new DeviceNet network configuration.		OK	OK
	EtherNet/IP	Creates a new EtherNet/IP network configuration.		OK	OK
	NE2A_Backplane	Creates a new NE2A Backplane configuration.		OK	OK
Open		Opens an existing network configuration file.		OK	OK
Save		Saves an existing network configuration file.		OK	OK

Menu commands		Description	Toolbar icon	Offline	Online
Save As		Saves the current network configuration under a new name. You can also use this command on version 3.3□ or higher to save a network configuration file in a format that can be used on version 2.	---	OK	OK
External data	Export Device List	Exports in CSV format a file with the device list that is displayed in the Network Configuration Pane.	---	OK	OK
	Export	Exports a network configuration file that can be used with Network Configurator version 2 or lower.	---	OK	OK
	Import	Imports network configuration files that were created with DeviceNet Configurator version 1 or version 2.	---	OK	OK
Change Password		Changes the password of the network configuration file. (Refer to *9-5-3 Password Protection for Network Configuration Files*.)	---	OK	OK
Report		Creates a report on a specified device.	---	OK	OK
Print		Prints the device parameters or I/O comment list. (Use the report function to print information for a Safety Device.)		OK	OK
Setup Printer		Sets up the printer.	---	OK	OK
Exit		Exits the Network Configurator.	---	OK	OK

Edit Menu

Menu commands	Description	Toolbar icon	Offline	Online
Cut	Deletes selected devices and copies them to the clipboard.		OK	OK
Copy	Copies selected devices to the clipboard.		OK	OK
Paste	Pastes a device on the clipboard to the cursor position.		OK	OK
Delete	Deletes selected devices.		OK	OK
Select All	Selects all devices.	---	OK	OK
Clear Message Report	Clears messages in the Message Report Pane.	---	OK	OK

View Menu

Menu commands		Description	Toolbar icon	Offline	Online
Toolbar	Generic	Displays or hides the standard toolbar.	---	OK	OK
	Device	Displays or hides the device toolbar.	---	OK	OK
	EDS	Displays or hides the EDS toolbar.	---	OK	OK
Status Bar		Displays or hides the status bar.	---	OK	OK
Message Report		Displays or hides the Message Report Pane.	---	OK	OK
Maintenance		Displays or hides the Maintenance Pane.	---	OK	OK
Large Icons		Switches the display to Normal Mode.		OK	OK
Large Icons - Maintenance Mode		Switches the display to Maintenance Mode.		OK	OK
Display Mode 1		Switches the display to Detailed Display Mode 1, which displays the configuration based on the Master.		OK	OK
Display Mode 2		Switches the display to Detailed Display Mode 2, which displays the configuration based on the Slaves.		OK	OK
Expand All Device		Displays the devices registered to the Master and Slaves in a detailed display.		OK	OK
Collapse All Device		Closes the display of the devices registered to the Master and Slaves in the detailed display.		OK	OK
Hardware List		Displays or hides the Hardware List Pane.	---	OK	OK
Network Structure		Displays or hides the Network Configuration List Pane.	---	OK	OK

Network Menu

Menu commands		Description	Toolbar icon	Offline	Online
Connect		Connects the Network Configurator to the network.		OK	---
Disconnect		Disconnects the Network Configurator from the network.		---	OK
Change Connect Network		Changes the destination network port.		---	OK
Wireless Network	Move to Upper Network	Displays the network one layer above the current network in the wireless networks. (Not normally used with the NE2A-series Controllers.)		---	OK
	Move to Lower Network	Displays the network one layer below the current network in the wireless networks. (Not normally used with the NE2A-series Controllers.)		---	OK
Upload		Uploads all the device parameters in the network to the Network Configurator.		---	OK
Download		Downloads all the device parameters in the Network Configurator to the devices in the network.		---	OK
Verify Structure		Verifies the current network configuration in the Network Configurator with the actual network configuration of the destination online connection.	---	---	OK
I/O connection	Start	Starts Safety I/O Communications for all Communications Units or individual Communications Units.	---	---	OK
	Stop	Stops Safety I/O Communications for all Communications Units or individual Communications Units.	---	---	OK
Update Maintenance Information		Updates the maintenance information of each device to the latest information.		---	OK

Menu commands		Description	Toolbar icon	Offline	Online
Update Device Status		Updates the status information of each device to the latest information.	---	---	OK
Connection Structure	Export	Exports the EtherNet/IP Tag Data Link connection settings to a file.	---	OK	OK
	Import	Imports the EtherNet/IP Tag Data Link connection settings from a file.	---	OK	OK
Auto Connection		Automatically sets the EtherNet/IP Tag Data Link connection settings.	---	OK	OK
View Device's Connection Structure Tree		Displays the connection configuration of the entire system.	---	OK	OK
Check Connection		Checks the consistency of all the connections.	---	OK	OK
Edit All Connections					
Add	DeviceNet	Adds a DeviceNet network in the Network Configuration Pane.	---	OK	OK
	EtherNet/IP	Adds an EtherNet/IP network in the Network Configuration Pane.	---	OK	OK
	NE2A_Backplane	Adds an NE2A_Backplane in the Network Configuration Pane.	---		
Copy		Copies the selected network configuration.	---	OK	OK
Delete		Deletes the selected network configuration.	---	OK	OK
Change View		Switches the displayed network.	---	OK	OK
Property		Displays the network properties. The network name and Safety Network number can be set. This function can also get network numbers from actual networks when the Network Configurator is online.	---	OK	OK

Device Menu

Menu commands		Description	Toolbar icon	Offline	Online
Parameter	Wizard	Configures the device parameters in a wizard format. This function is not supported by all devices.		OK	OK
	Edit	Edits the device parameters.		OK	OK
	Open	Reads the parameters from the device parameter file.		OK	OK
	Save As	Saves the device parameters to a file.		OK	OK
	Upload	Uploads the device parameters from a device in the network.		---	OK
	Download	Downloads the device parameters to a device in the network.		---	OK
	Verify	Verifies the device and the device parameters in the network.		---	OK
	Lock	Locks the configuration of a device in the network.	---	---	OK
	Unlock	Unlocks the locked configuration of a device in the network.	---	---	OK
Monitor		Monitors the parameters and status of a device in the network. Not all devices support this function.		---	OK
Reset		Resets a device in the network.	---	---	OK

Menu commands		Description	Toolbar icon	Offline	Online
Change Mode	Idle	Changes the status of a device in the network. Not all devices support this function.	---	---	OK
	Execute	Changes the status of a device in the network. Not all devices support this function.	---	---	OK
Change Password		Changes the password of a device in the network.	---	---	OK
Set TUNID		Sets the TUNID for network devices. (Version 3.3□ or higher)	---	---	OK
Maintenance Information		Displays the maintenance information of a device in the network. Not all devices support this function.		---	OK
Register to other Device		Registers a device to another device.	---	OK	OK
External Data	Export	Exports I/O comments or device parameters to another file format. Not all devices support this function.	---	OK	OK
	Import	Imports a device parameter file created with DeviceNet Configurator version 1 or 2. Not all devices support this function.	---	OK	OK
	Create Configuration Restore File	Creates a file that can be used to restore the configuration.	---	OK	OK
Change Node Address		Changes a device node address.	---	OK	OK
Change Device Comment		Changes a device name.	---	OK	OK
Change Device		Converts configuration data for the NE1A-SCPU01 to configuration data for the NE1A-SCPU01-V1 or NE1A-SCPU02.	---	OK	OK
Edit I/O Comment		Edits the I/O comment.		OK	OK
Synchronize Identity		A new network can be created (or selected from existing networks), and the routing destination network can be specified.	---	OK	OK
Register to Routing Network					
Display Routing Network					
Property		Displays the properties of a device.		OK	OK

Note The some of the commands from the Device Menu and Edit Menu can be displayed by right-clicking in the Network Configuration Pane.

EDS File Menu

Menu commands	Description	Toolbar icon	Offline	Online
Install	Installs an EDS file and adds a device to the Hardware List. (Normally there is no need to install the EDS files.)		OK	OK
Create	Creates a new EDS file and adds a device to the Hardware List.	---	OK	OK
Delete	Deletes a device from the Hardware List. The installed EDS file is also deleted.		OK	OK
Save As	Names and saves the EDS file of a device on the Hardware List.		OK	OK
Find	Searches for a specified EDS file from the Hardware List.		OK	OK
Add to Network	Adds a device on the Hardware List to the virtual network.		OK	OK

Menu commands	Description	Toolbar icon	Offline	Online
Property	Displays the properties of an EDS file.		OK	OK
Create EDS Index File	Recreates the EDS index file. If the devices are not correctly displayed in the Hardware List Pane, restart the Network Configurator. (Version 3.3□ or higher)	---	OK	OK

Note The EDS File Menu can be displayed by right-clicking in the Hardware List Pane.

Note Start the Network Configurator as the system administrator to install, create, or delete EDS files or create EDS index files. (Refer to *9-4-1 Starting and Exiting the Network Configurator*.)
On Window 2000 or XP, these operations are not possible unless you are logged on with administrator rights.
On Windows Vista or 7, if the above operations are preformed when the Network Configurator is started without administrator rights, Windows Vista/7 user account management will redirect you to the local folder of the user that started the Network Configurator. The results of these operations will therefore not be applied for other user accounts.

Tools Menu

Menu commands	Description	Toolbar icon	Offline	Online
Setup Parameters	Sets parameters by using explicit message communications.	---	---	OK
Setup Node Address/Baud Rate (only when DeviceNet is selected)	Sets the node address and baud rate of a device in the DeviceNet network.	---	---	OK
Setup TCP/IP Configuration (only when EtherNet/IP is selected)	Makes TCP/IP settings, such as the IP address and subnet mask of a device on an EtherNet/IP network.	---	---	OK

Option Menu

Menu commands	Description	Toolbar icon	Offline	Online
Select Interface	Selects an interface for the Network Configurator to use for the network connection.	---	OK	---
Edit Configuration File	Edits various setup files. (Normally not required.)	---	OK	OK
Setup Monitor Refresh Timer	Sets the monitor refresh timer values (monitoring cycles in device monitoring).	---	OK	OK
Install Plug-in Module	Installs a Plug-in Module. (Normally not required.)	---	OK	OK
Install Interface Module	Installs an Interface Module. (Normally not required.)	---	OK	---
Update Parameter automatically, when Configuration was Changed	The Slave parameters registered in the Master will be updated automatically when a Slave parameter is changed. This options is cleared by default (do not update). Under normal conditions, do not select this option.	---	OK	OK
Update Device Status automatically, when it was connected on Network	When this option is selected and the device is online, its status will be automatically detected and displayed.	---	OK	---

Note To edit the configuration file, install a plug-in module, or install an interface module, start the Network Configurator as the system administrator. (Refer to *9-4-1 Starting and Exiting the Network Configurator*.)
On Window 2000 or XP, these operations are not possible unless you are logged on with administrator rights.
On Windows Vista or 7, if the above operations are preformed when the Net-

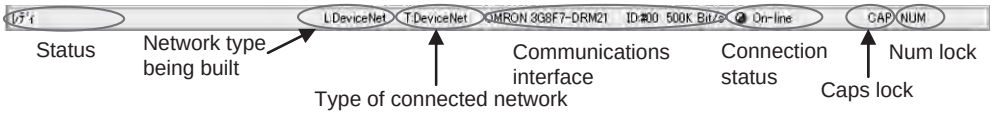
work Configurator is started without administrator rights, Windows Vista/7 user account management will redirect you to the local folder of the user that started the Network Configurator. The results of these operations will therefore not be applied for other user accounts.

Help Menu

Menu commands	Description	Toolbar icon	Offline	Online
Topic	Searches the help topics.	---	OK	OK
About	Displays the Network Configurator version information.	---	OK	OK

IMPORTANT The Network Configurator does not provide a lockout function to disable operation if no operations are performed for a specific period of time. If a lockout function is required, use the password protection function for the screen saver provided by Microsoft Windows.

9-6-5 Status Bar



The following table describes the information displayed on the status bar.

Name	Description
Status	Indicates the Network Configurator status and gives a description of the menu and toolbar A menu description or toolbar icon description is displayed when the mouse is moved to a menu or toolbar icon.
Network type being built (L:)	Displays the network type (DeviceNet, EtherNet/IP, or NE2A_Backplane) of the network in the Network Configuration Pane.
Type of connected network (T:)	Displays the network type of the connected main network (DeviceNet, EtherNet/IP, or NE2A_Backplane). “Unknown” will be displayed when offline.
Communications interface	Displays details on the interface used for the connection. For further information, refer to the following table.
Connection status	Indicates the connection status of the Network Configurator to the network. On-line: The blue icon indicates that the Network Configurator is connected to the network. Off-line: The gray icon indicates that the Network Configurator is not connected to the network.
Caps Lock	“CAP” will be displayed when the Caps Lock Key is ON; nothing will be displayed when the Caps Lock Key is OFF.
Num Lock	“NUM” will be displayed if the Num Lock Key is ON; nothing will be displayed when the Num Lock Key is OFF.

The following table shows the information that is displayed for the communications interface.

Interface	Description
CJ2 USB/Serial Port	Communications port: Network connection name Network device name Baud rate
NE1S Serial Port	Communications port: Network connection name Network device name Baud rate
CS/CJ1 Serial Port to DRM Unit Interface	Communications port: Network connection name Network device unit number Baud rate
Ethernet to CS/CJ1 ETN/DRM Unit Interface	Network device name Node ID IP address of local computer Baud rate Network device unit number Network device IP address
DeviceNet Interface	Network device name Board ID Baud rate
EtherNet Interface	Ethernet interface IP address of local computer
RSLinx Interface	RS-Linx interface: Set interface name.
NExA USB Port	Communications port: Network connection name Network device name Baud rate

SECTION 10
Designing the System Configuration

This section describes the settings for the NE2A-series Safety Network Controller and other device parameters.

10-1 NE2A-series Controller Setup 232
10-1-1 Creating the NE2A Backplane 232
10-1-2 Registering the CPU Unit 234
10-2 Setting Device Parameters 235
10-2-1 Mode/Cycle Times 236
10-2-2 Extend Mode 236

10-1 NE2A-series Controller Setup

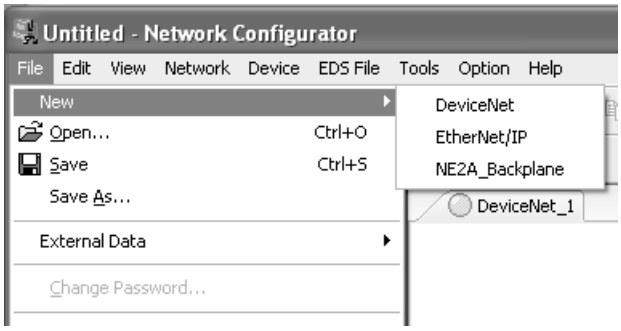
This section describes how to register the NE2A-series CPU Unit to a project, and how to set the I/O Unit configuration and parameters in the CPU Unit.

10-1-1 Creating the NE2A Backplane

With the Network Configurator, create an NE2A Backplane as a virtual network to register the NE2A-series Units. The NE2A Backplane serves as a virtual network for linking the CPU Unit to DeviceNet Units and EtherNet/IP Units.

Creating or Adding an NE2A Backplane

Create an NE2A Backplane virtual network.

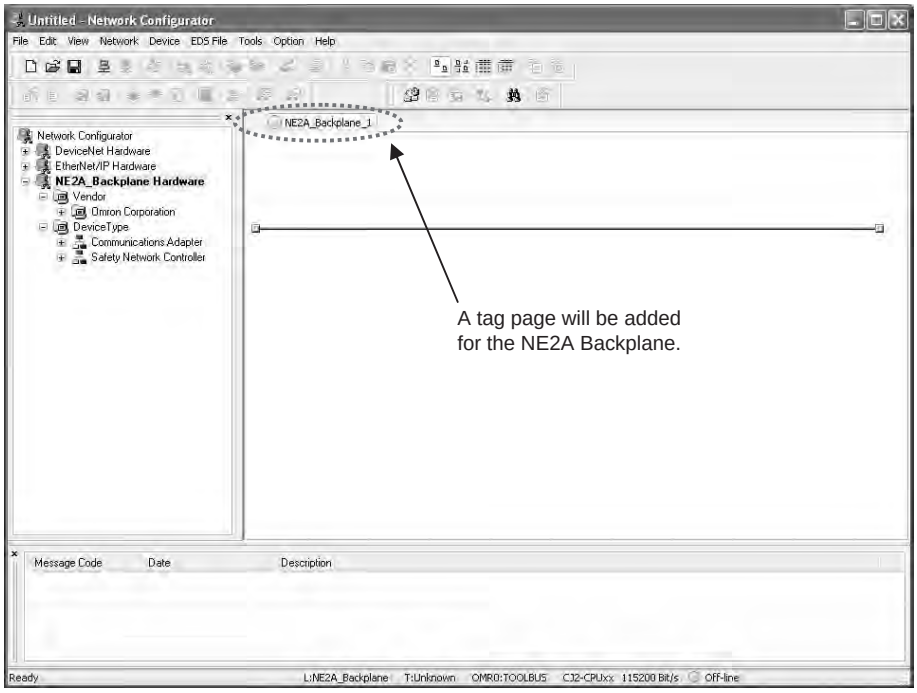


Procedure

To create a new Backplane, select ***New - NE2A_Backplane*** from the File Menu.

To add a network, select ***Add - NE2A_Backplane*** from the Network Menu.

An NE2A_Backplane_1 Tab Page will be created in the Network Configuration Pane.



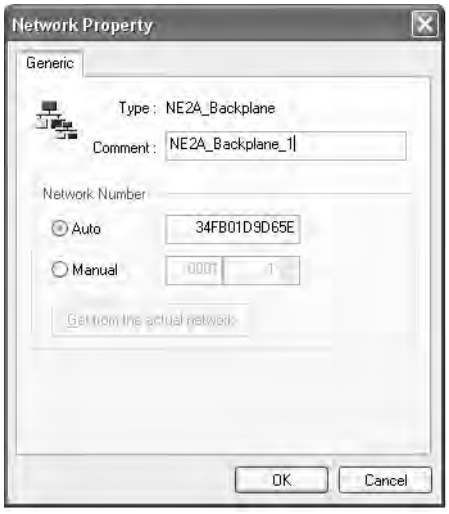
Setting the Network Number

Network numbers are used to uniquely identify devices and perform mutual confirmation when multiple networks are set. The system uses TUNIDs (Target Unique Network Identifiers, which are IDs that combine the network number and the device node address to uniquely identify the device. For details, refer to *5-2-2 DeviceNet Communications.*

Network Number Settings

1,2,3... 1. Select *Properties* from the Network Menu.

The Network Property Dialog Box will be displayed.



2. Select *Manual User Specified* for the network number and enter a value.
3. Click the **OK** Button to set the network number.

An error message will be displayed if the specified network number is the same as one for another network.



Note A connection with an unintended device may be established if the network number is not set correctly. Set a different network number value for each network domain and always set the same network number for all devices on the same domain.

Checking the Network Number

Use the following procedure to check the network number set for the actual network.

1,2,3... 1. Select *Properties* from the Network Menu.

The Network Properties Dialog Box will be displayed.

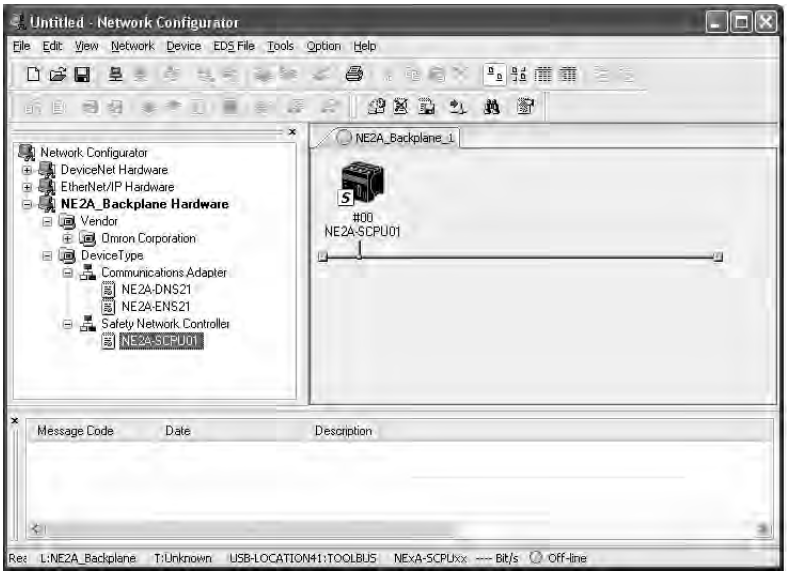
2. Click the **Get from the actual network** Button.

The network number set for the targeted actual network will be read and displayed in the *Network Number* Column.

10-1-2 Registering the CPU Unit

Registering the CPU Unit

Double-click ***NE2A-SCPU01*** under ***NE2A_Backplane Hardware - Device Type - Safety Network Controller*** in the Hardware List Pane.



The NE2A-series CPU Unit will be registered to the Backplane.

Changing the Device Name

Device names can be changed.

When a device is added from the Device List, the displayed name is the name that is used in the Device List.

Procedure

1,2,3...

1. Select the device for which the name will be changed.
2. Select *Change Device Comment* from the Device Menu.
   Or, right-click the device and select *Change Device Comment*.
   The Change Device Comment Dialog Box will be displayed.



3. Enter a device name and click the **OK** Button.

Note Up to 32 alphanumeric characters can be entered as the device name.

10-2 Setting Device Parameters

This section describes how to set the parameters for devices set for the NE2A-series CPU Unit.

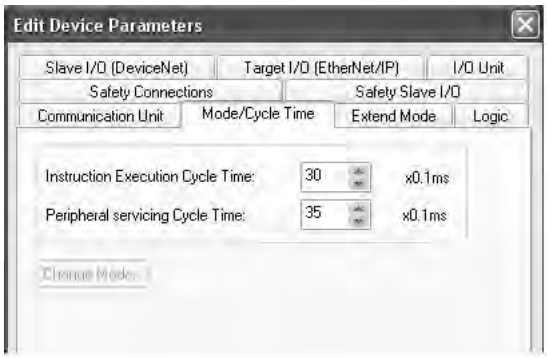


Tab page	Description
Safety Connections	Used to set the Safety Connections. Refer to *Sections 11* and *12*.
Safety Slave I/O	Used to create and display the assembly data when the applicable NE2A-series Controller communicates over DeviceNet and EtherNet/IP networks as a Safety Slave. Refer to *Sections 11* and *12*.
Slave I/O (DeviceNet)	Used to create and display the assembly data when the applicable NE2A-series Controller communicates over a DeviceNet network as a Standard Slave. Refer to *Section 11*.
Target I/O (EtherNet/IP)	Used to create and display the assembly data for when the applicable NE2A-series Controller communicates over an EtherNet/IP network as a Target. Refer to *Section 12*.
I/O Unit	Used to set the I/O Units to be mounted to the CPU Unit. Refer to *Section 14*.
Communications Unit	Used to set the Communications Units (DeviceNet and EtherNet/IP) to be mounted to the CPU Unit. Refer to *Section 11*.
Mode/Cycle Time	Used to display the instruction execution cycle time and the peripheral servicing cycle time. Refer to *10-2-1 Mode/Cycle Times*.
Extend Mode	Used to set the program execution delay time, restore operation settings, RUN/IDLE operation settings, user program ID, and parameter protection. Refer to *10-2-2 Extend Mode*.
Logic	Used to start the Logic Editor for program development. Refer to *Section 15*.

10-2-1 Mode/Cycle Times

■ Cycle Times

Set the cycle times (the instruction execution cycle time and the peripheral servicing cycle time) for system operation.



■ Changing the Mode

The operating mode can be changed between IDLE and RUN if the Network Configurator is connected online to the NE2A-series Controller.

10-2-2 Extend Mode

Program Execution Delay Time

- Disable: Execute the program without waiting for Safety I/O Communications to start.
- Enable: Wait for Safety I/O Communications to start before executing the program.

Restore Operation Mode

This parameter sets the devices for the configuration restore operation.

- This device only: The configuration is restored only for the selected NE2A-series Controllers.
- All devices on the network: The configuration is restored for all NE1A-series and NE0A-series Controllers on the DeviceNet networks of the selected NE2A-series Controller.

Run/Idle Operation Mode

This parameter sets the devices for which the operating mode is to be changed for the configuration restore operation.

- This device only: The operating mode is changed only for the selected NE2A-series Controllers.
- All devices on the network: The operating mode is changed for all NE1A-series and NE0A-series Controllers on the DeviceNet networks of the selected NE2A-series Controller.

User Program ID

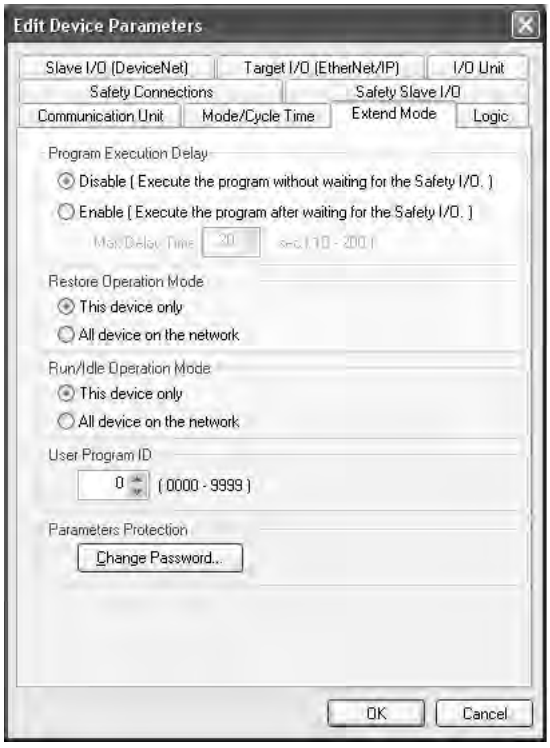
Set any 4-digit number for the user program. The value that is set will be displayed on the 7-segment display on the CPU Unit (except when an error is being display, when checking an operation authorization file, or when in Configuration Restore Mode).

Parameter Protection

A password for editing and a password for browsing can be used to prevent editing and browsing by unauthorized users.

The passwords described here protect the following items.

- Device parameters
- Programming



SECTION 11
Setting DeviceNet Networks

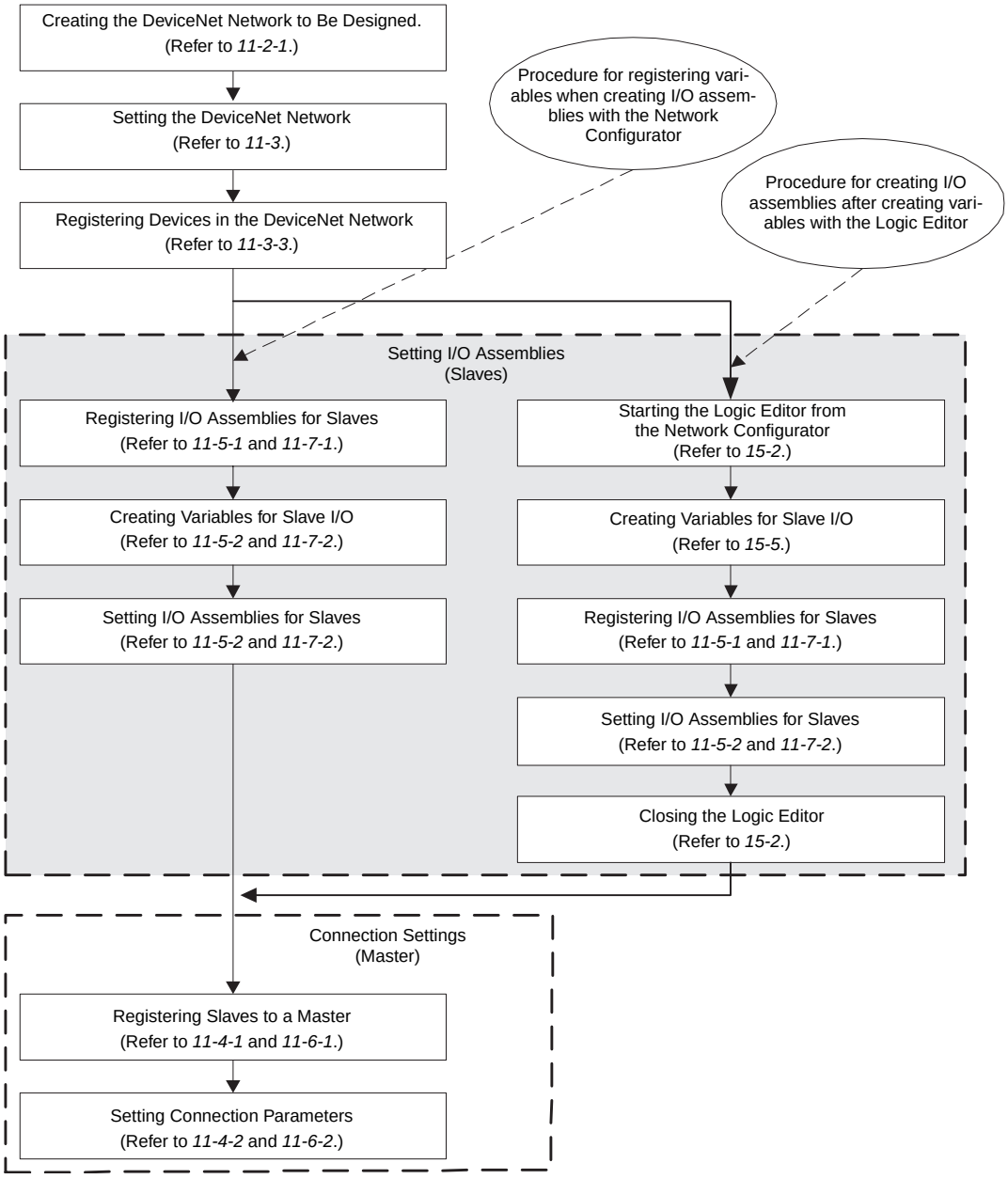
This section describes how to set up DeviceNet networks for a NE2A-series Safety Network Controller.

11-1 DeviceNet Network Setting Procedure 240
11-2 Registering DeviceNet Units to the CPU Unit 241
11-2-1 Associating the CPU Unit and DeviceNet Units 241
11-3 DeviceNet Network Settings 245
11-3-1 Setting Network Addresses 245
11-3-2 Setting Node Addresses 246
11-3-3 Adding Devices to a Network 246
11-4 Communications between an NE2A-series Controller and a Safety Slave . . . 249
11-4-1 Registering Safety Slaves 249
11-4-2 Setting Safety Connection Parameters 254
11-4-3 Convenient Functions for Editing Connections 256
11-4-4 Stopping or Restarting Communications after an Error 258
11-5 Using the NE2A-series Controller as a Safety Slave 259
11-5-1 Registering I/O Assemblies for Safety Slaves 259
11-5-2 Setting Assembly Data 263
11-5-3 Registering I/O Assemblies from the Logic Editor 267
11-6 Communications between the NE2A-series Controller and Standard Slaves . 269
11-6-1 Registering Standard Slaves 269
11-6-2 Setting Standard Connections 271
11-7 Using an NE2A-series Controller as a Standard Slave 273
11-7-1 Registering I/O Assemblies for Standard Slaves 273
11-7-2 Setting Assembly Data 276
11-7-3 Registering from the Logic Editor 277
11-7-4 Setting Slave Input Data in IDLE Mode 277
11-8 Communications between an NE2A-series Controller and a Standard Master 278

11-1 DeviceNet Network Setting Procedure

This section describes how to build and set a DeviceNet network to perform DeviceNet communications. With NE2A-series Controllers, any of the following functions can be allocated to each DeviceNet Unit: Safety Master, Safety Slave, Standard Master, or Standard Slave.

The Slave procedure is not required if the NE2A-series Controller will not be used as a Safety Slave or Standard Slave.



11-2 Registering DeviceNet Units to the CPU Unit

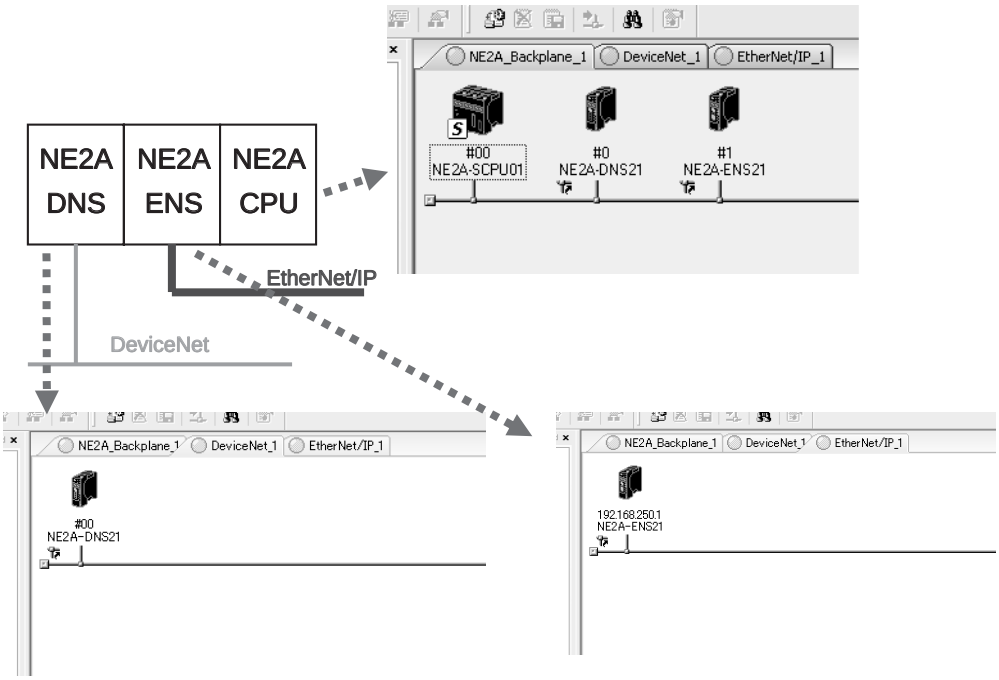
This section describes the procedure for registering DeviceNet Units to an NE2A-series CPU Units to build a DeviceNet network.

11-2-1 Associating the CPU Unit and DeviceNet Units

An NE2A-series CPU Unit does not have a communications port for DeviceNet or EtherNet/IP communications. To perform DeviceNet or EtherNet/IP communications, mount an NE2A-DNS21 DeviceNet Unit or an NE2A-ENS21 EtherNet/IP.

To associate these Communications Units with a CPU Unit, register them to the NE2A-series Backplane of the CPU Unit.

The following figure shows display examples of the Unit configuration in the Network Configurator.

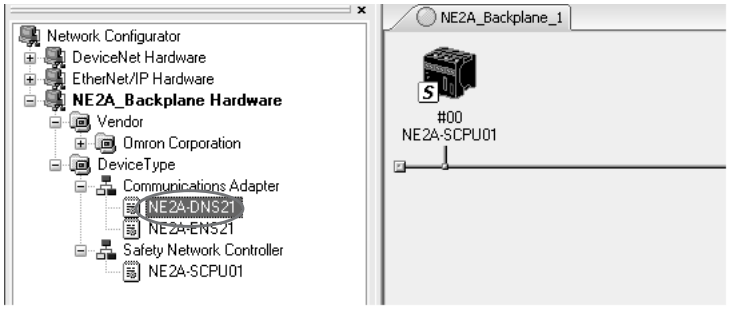


Registering DeviceNet Units

Register the NE2A-DNS21 DeviceNet Unit to the NE2A-series Backplane.

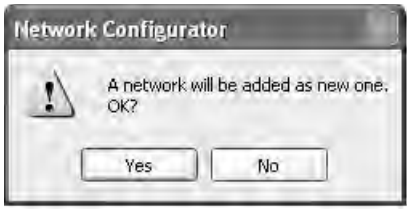
Procedure

1,2,3... 1. Double-click *NE2A-DNS21* in the Hardware List Pane. You can also drag *NE2A-DNS21* from the Hardware List Pane and drop it in the Network Configuration Pane.

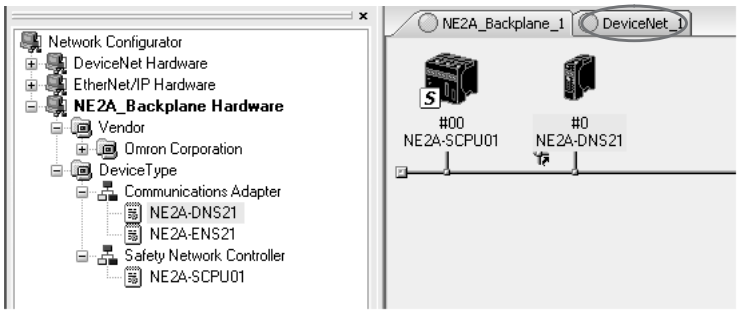


2. Select the NE2A-DNS21 added in step 1.

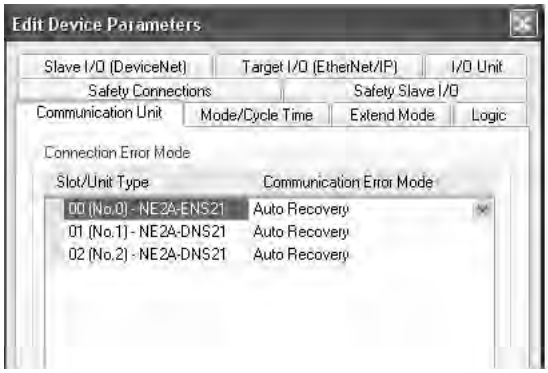
3. Select ***Register to Routing Network*** from the Device Menu.
   You can also right-click the NE2A-DNS21 and select ***Register to Routing Network*** from the menu.
   A dialog box will be displayed to confirm whether to add to the network.



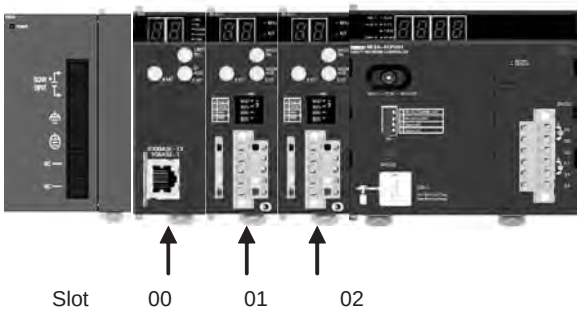
4. Click the **Yes** button.
   A DeviceNet Tab will be added to the Network Configuration Pane.



Note The slot numbers of the device parameters will be assigned in the order that the Communications Unit is added to the NE2A Backplane. Change the slot number to match the actual configuration by using the tab page for the Communications Unit in the Edit Device Parameters Dialog Box. This dialog box is displayed by selecting ***Parameter - Edit*** from the Device Menu. Change the slot arrangement of the Communications Unit by pressing the **Up** Button or **Down** Button.

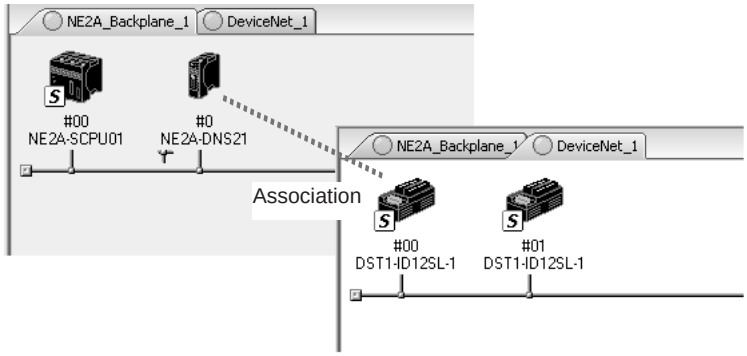


Slot numbers are assigned in order (00, 01, etc.) to Communications Units from the right side of the Power Supply Unit.



Associating an NE2A-series Backplane with Other Networks

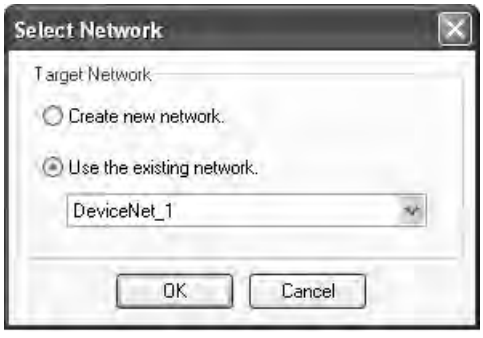
Associations can be made to the NE2A-series Backplane after creating the DeviceNet network.



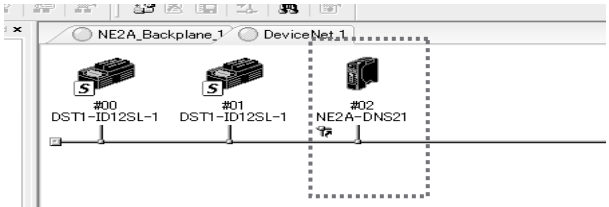
Procedure

1,2,3...

1. Add a NE2A-DNS21 to the NE2A-series Backplane of the NE2A-series Controller.
2. Select the NE2A-DNS21.
3. Select ***Register to Routing Network*** from the Device Menu.
   You can also right-click the NE2A-DNS21 and select ***Register to Routing Network*** from the menu.
   The Select Network Dialog Box will be displayed.



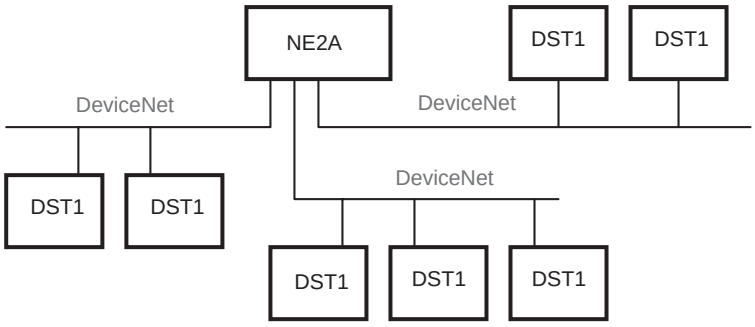
4. Select the *Use the existing network* Option and select the network name to be associated.
5. Click the **OK** Button.
   The network associations will be made.



The NE2A-DNS21 will be added to the network.

11-3 DeviceNet Network Settings

More than one Communications Unit can be connected in an NE2A-series Controller, so it is often necessary to manage multiple networks. This section describes how to make settings for network numbers and node addresses to manage DeviceNet networks.



11-3-1 Setting Network Addresses

Here we will make the settings for the DeviceNet network created in *11-2-1 Associating the CPU Unit and DeviceNet Units*.

Network Numbers

Network numbers are used in configurations with more than one DeviceNet network to uniquely identify devices.
To uniquely identify devices, a Target Unique Network Identifier (TUNID) value that combines the network number and the device node address is used.
For details, refer to *5-2-2 DeviceNet Communications*.

Setting Network Numbers

1,2,3... 1. Select ***Properties*** from the Network Menu.
The Network Property Dialog Box will be displayed.



2. Select the *Manual* Option in the Network Number Area and enter a value.
3. Click the **OK** Button to set the network number.
An error message will be displayed if a network number that is already used for other network is set.



Note If the network number is set incorrectly, a connection may be opened with an unintended device. Set a different network number for each network domain and always set the same network number for all devices on the same network domain.

Checking Network Numbers

Use the following procedure to check the network numbers set for networks before you set a network number.

1,2,3...

1. Select ***Properties*** from the Network Menu.
   The Network Property Dialog Box will be displayed.
2. Click the **Get from the actual network** Button.
   The network number of the network will be read and displayed in the *Manual* Field.

11-3-2 Setting Node Addresses

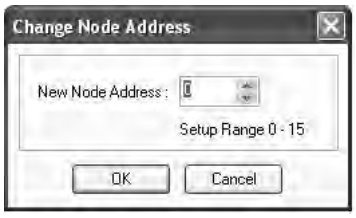
When a device is added to a virtual network, an unused node address from 0 to 63 will be automatically allocated in the order that the device is added.

Set the node addresses so that they match the rotary switches on the NE2A-DNS 21 DeviceNet Unit.
Refer to *3-6-3 Switches* for information of setting node addresses using the rotary switches.

Procedure

1,2,3...

1. Select the device in the Network Configurator and select ***Change Node Address*** from the Device Menu.
   You can also right-click the device in the Network Configurator and select ***Change Node Address***.
   The Change Node Address Dialog Box will be displayed.



2. Change the node address and click the **OK** button.

Note A node address duplication error will occur if the node address is the same as one used for another node. If this error occurs, communications will not start.

11-3-3 Adding Devices to a Network

There are three ways to add devices to a virtual network.

- Adding a device from the Hardware List Pane (Refer to *Adding Devices from the Hardware List*, below.)
- Obtaining the network configuration from the actual network (Refer to *17-3-2 Uploading Device Parameters*.)

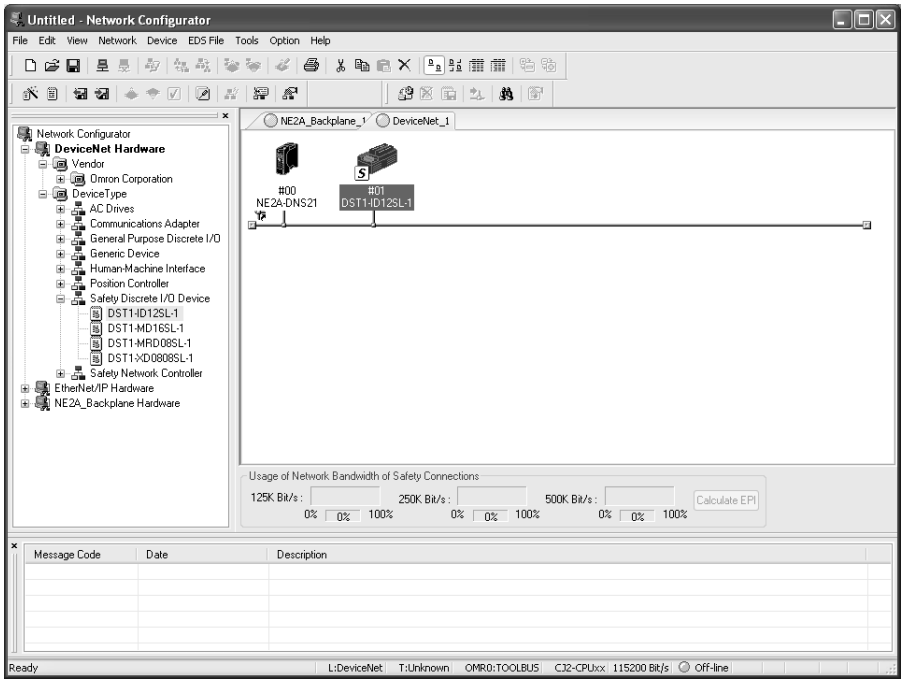
- Selecting ***Add to Network*** from the EDS File Menu

Adding Devices from the Hardware List

Use the following procedure to add a device from the Hardware List Pane to the virtual network.

Procedure

Double-click the device in the Hardware List Pane and drag it to the Network Configuration Pane.
The following display will appear when the device is registered.

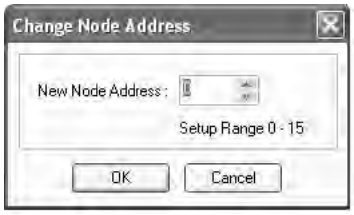


Changing Device Addresses

Allocated node addresses can be changed. When a device is added, and unused node address from 0 to 63 will be automatically allocated in the order that the device is added.
Set the node addresses so that they match the rotary switches on the devices added. (Refer to the manual of the relevant device for information on how to set the rotary switches.)

Procedure

1,2,3... 1. Select the device and select ***Change Node Address*** from the Device Menu.
You can also right-click the device and select ***Change Node Address***.
The Change Node Address Dialog Box will be displayed.



2. Change the node address and click the **OK** Button.
   Set the node address so that it matches the rotary switches on the DeviceNet Unit.
   An error message will be displayed if an attempt is made to set a node address that is being used by another device.



Changing the Device Name

You can change the name of a device. When you add a device from the Device List, the name that is displayed will be the name from the Device List.

Procedure

1,2,3... 1. Select the device and then select ***Change Device Comment*** from the Device Menu.
   You can also right-click the device and select ***Change Device Comment***.
   The Change Device Comment Dialog Box will be displayed.



2. Enter a device name and click the **OK** Button.

Note Up to 32 characters can used for the device name.

Deleting a Device

It is possible to delete a device from the virtual network.

Procedure

1,2,3... 1. Select the device and select ***Delete*** from the Edit Menu.
   You can also select the device and click the **Delete** Button on the toolbar.
   Or, right-click the device and select ***Delete***.
   A dialog box will be displayed to confirm the deletion.



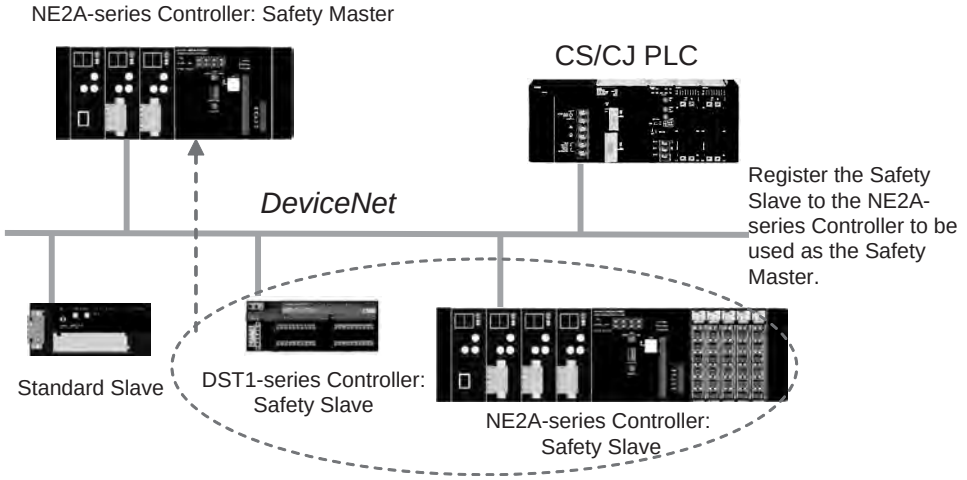
2. Press the **Yes** Button to delete the device.

11-4 Communications between an NE2A-series Controller and a Safety Slave

This section described how to make settings to perform communications with a Safety Slave using an NE2A-series Controller as a Safety Master in a DeviceNet network.
To operate the NE2A-series Controller as a Safety Master, register the device that is to operate as a Safety Slave and set the connection.

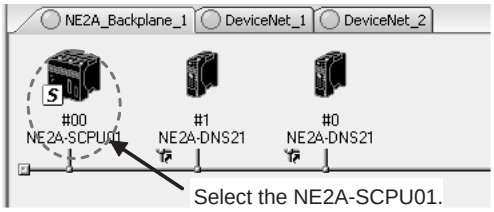
11-4-1 Registering Safety Slaves

Register the Safety Slave to communicate with and set the connection.
Refer to *11-3 DeviceNet Network Settings* for information on how to build a DeviceNet network.
This section describes how to set a Safety Connection with a DeviceNet network that has already been built. Refer to *5-4-2 Setting Safety Connections* for information on Safety Connections.



Procedure

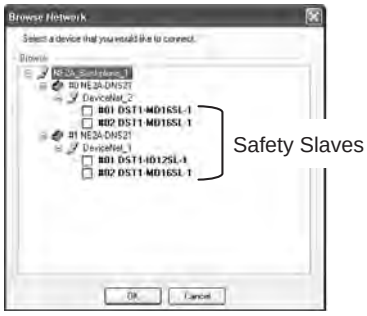
1,2,3... 1. Select the NE2A-SCPU01 to set in the NE2A Backplane Tab Page of the Network Configuration Pane.



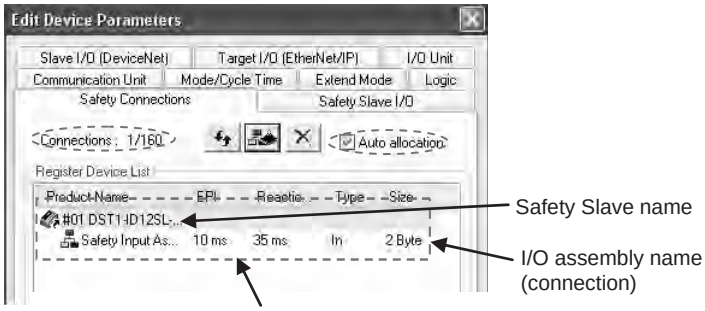
2. Select ***Parameters - Edit*** from the Device Menu.
   You can also right-click the NE2A-SCPU01 device and select ***Parameters - Edit*** from the menu.
   Or, you can double-click the NE2A-SCPU01 device.
   The Edit Device Parameters Dialog Box will be displayed.



3. Click the **Browse Network** Button ( ).
   The Browse Network Dialog Box will be displayed.



4. Select the Safety Slave and click the **OK** Button.
   The Safety Slave will be displayed in the Register Device List Area on the Safety Connections Tab Page in the Edit Device Parameter Dialog Box.



The following information is displayed in the list of registered devices.

Item	Description
Product Name	The name of the registered Safety Slave (icon) and the name of the I/O assembly used in the set Safety Connection (icon) are displayed.
EPI	The EPI of the Safety Connection is displayed. Refer to *11-4-2 Setting Safety Connection Parameters* for information on the EPI.
Reaction Time	The network response time of the Safety Connection is displayed.

Item	Description
Type	The type of I/O assembly used by the Safety Connection is displayed. In: Input assembly (Slave to Master) Out: Output assembly (Master to Slave)
Size	The size of I/O assembly data used by the Safety Connection is displayed.

- Here the *Auto allocation* Option is selected at the upper-right of the tab page, so the default connection (I/O assembly) of the Safety Slave will be registered when the Safety Slave is registered. (If this option is not selected, the connection will not be registered and the name of the I/O assembly will not be displayed.)
- The number of connections over the number of connections that can be used is displayed in the upper-left part of the tab page.

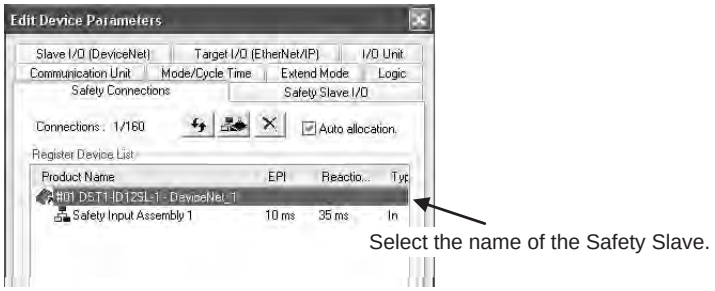
Note (1) A maximum of 160 connections can be registered. (A maximum of 64 connections that can be set for one DeviceNet Unit.)

(2) If an NE2A-series Controller is set as a Safety Slave, the default I/O assembly will not be set.

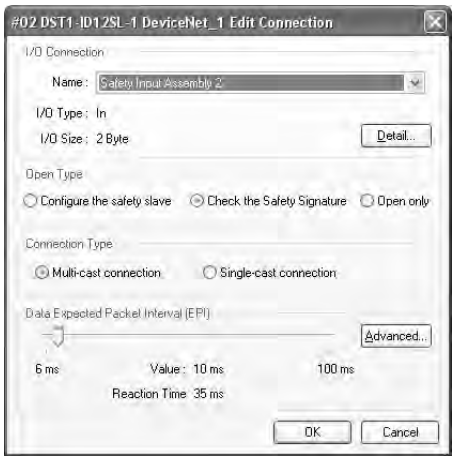
Adding Connections

Procedure

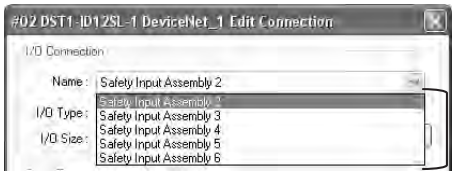
1,2,3... 1. Select the name of the Safety Device for the connection to be added from the Register Device List Area on the Safety Connections Tab Page in the edit Device Parameters Dialog Box.



2. Click the **New** Button.
A dialog box will be displayed to register the connection for the device.

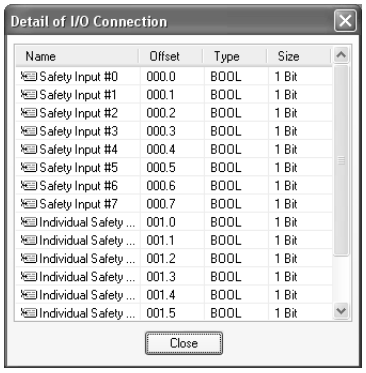


3. Select the connection name to be added.

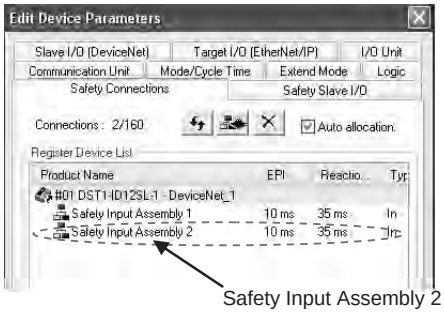


Select the assembly name displayed in the dropdown list.

4. Click the **Detail** Button to display detailed information on assemblies.



5. Set the connection parameters and click the **OK** Button. (Refer to *11-4-2 Setting Safety Connection Parameters* for information on parameters.)
The connection will be added in the Register Device List Area in the Edit Device Parameters Dialog Box.

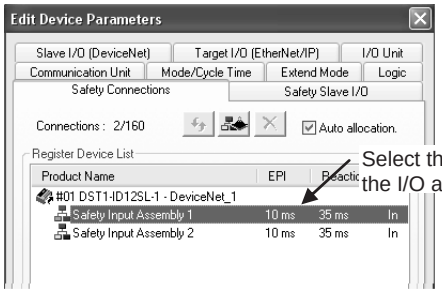


Safety Input Assembly 2 will be added.

Deleting Connections

Procedure

1,2,3... 1. Select the name of the I/O assembly to be deleted from the Register Device List Area on the Safety Connections Tab Page in the Edit Device Parameters Dialog Box.

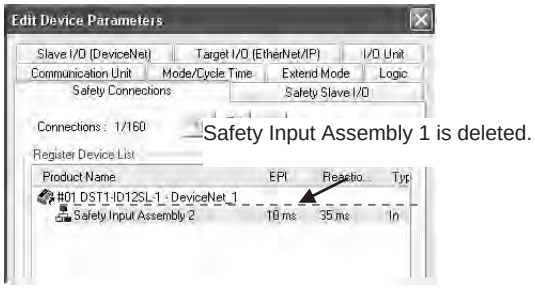


Select the name of the I/O assembly.

2. Click the **Delete** Button.
A dialog box will be displayed to confirm the deletion.



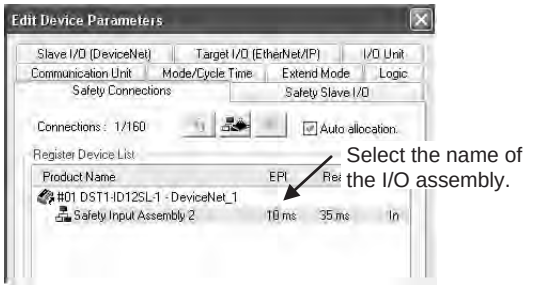
3. Click the **Yes** Button.
   The selected connection will be deleted.



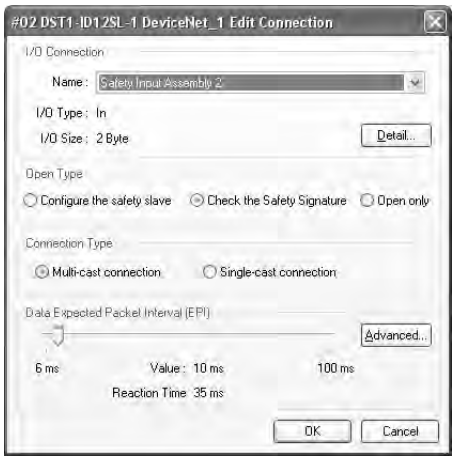
Editing Connections

Procedure

1,2,3... 1. Select the name of the I/O assembly to be edited from the Register Device List Area on the Safety Connections Tab Page in the Edit Device Parameters Dialog Box.



2. Click the **Edit** Button.
   A dialog box to register the connection to the device will be displayed.



3. Change the parameters and click the **OK** Button.
   For details, refer to *11-4-2 Setting Safety Connection Parameters*.

Automatically Registering and Unregistering Connections

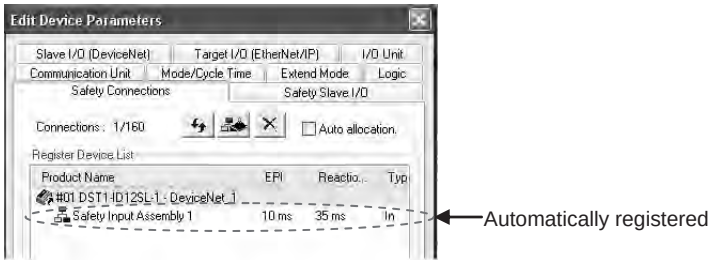
Procedure

1,2,3... 1. Select the name of the Safety Slave of the connection to be automatically registered or to be deleted from the Register Device List Area on the Safety Connections Tab Page in the Edit Device Parameters Dialog Box.

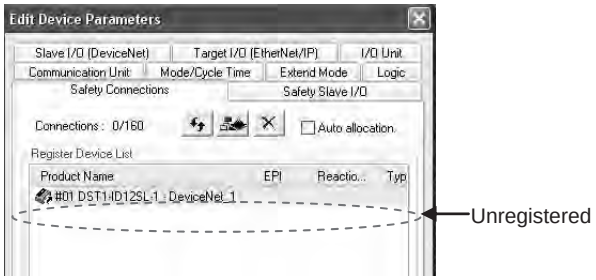


2. Click the **Register/Unregister** Button.
It is possible to unregister all connections if they have already been set and register the connections and the parameters for those connections if the connections have not been set.

Clicking the **Register/Unregister** Button when the Connection Is Not Registered:



Clicking the **Register/Unregister** Button when the Connection Is Registered:



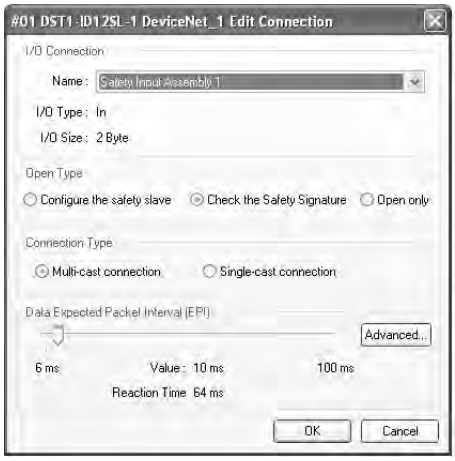
Note (1) To delete a Safety Slave from the Register Device List Area, select the Safety Slave to delete and click the **Delete** Button (✕).

(2) The program may be affected if a Safety Connection setting is changed. After making the change, open the Logic Editor and check the program.

11-4-2 Setting Safety Connection Parameters

This section describes how set Safety Connection parameters.

Make the settings in the dialog box to register the connection to the device.



I/O Connections

Select the I/O assembly to use from among the I/O assemblies for the Safety Slave to communicate with. The I/O assemblies that can be selected depend on the type of Safety Slave.

I/O connection	Description
Name	Used to select the I/O assembly to be used.
I/O type	The I/O type (input or output) of the I/O assembly is displayed.
I/O size	The I/O size of the I/O assembly is displayed.

Note Set the I/O assembly on the Safety Target I/O Tab Page to use the Safety Slave in the NE2A-series Controller. Refer to *11-5 Using the NE2A-series Controller as a Safety Slave*.

Open Type

Select the open type to use when the NE2A-series Controller establishes a connection with a Safety Slave.
For details, refer to *5-4-2 Setting Safety Connections*.

Note

(1) Do not select the *Configure the safety slave* Option in the Open Type Area.

(2) If the *Open only* Option is selected as the open type for the connection, be sure that the Safety Master and Safety Slave are configured correctly.

Connection Type

Select the connection type to use between the NE2A-series Controller and the Safety Slave.
For details, refer to *5-4-2 Setting Safety Connections*.

EPI

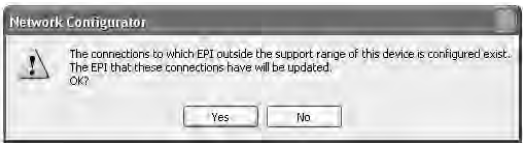
EPI is the interval at which the Safety Controller and Safety Slaves perform communications of safety data.
For details, refer to *5-4-2 Setting Safety Connections*.

Note

(1) Set the EPI for each Safety Connection that is longer than the cycle time of the Safety Network Controller. If the EPI is shorter, an error will occur and downloading will fail when an attempt is made to download the parameters for the Safety Connections.

(2) The Network Configurator can automatically adjust the EPI. The value can be changed automatically if the set EPI is shorter than the local cycle

time when the set EPI and local cycle time are compared. The following warning will be displayed if the value set for the EPI is smaller than the local cycle time.

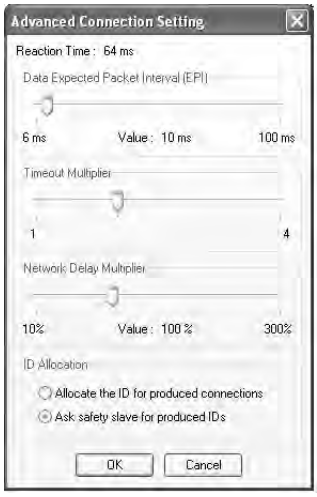


Click the **Yes** Button in the dialog box to automatically change the value of the relevant connection EPI to the same value as local cycle time. This allows you to prevent errors when downloading.

(3) The remote cycle time will not be checked if the device to communicate with is an NE2A/NE1A-series Controller (Slave operation). Check that the EPI that is set is equal to or greater than the cycle time of the remote NE2A/NE1A-series Controller.

Advanced Settings

Click the **Advanced Setup** Button to display the Advanced Connection Settings Dialog Box. The communications parameters can be changed, but normally there is no need to make changes. For details, refer to *5-4-2 Setting Safety Connections*.



11-4-3 Convenient Functions for Editing Connections

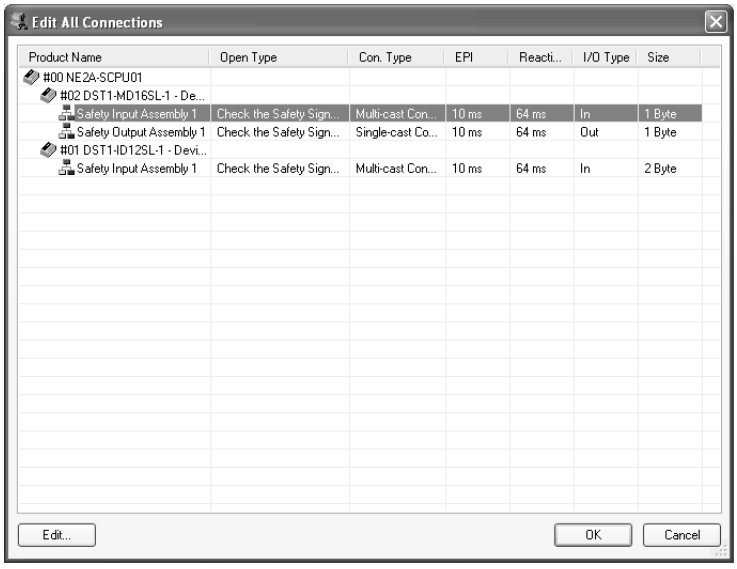
Editing All Connections

You can display the connection information for all currently set devices in a table and change the parameters. It is not possible to make new connections or to delete existing connections.

Procedure

1,2,3...

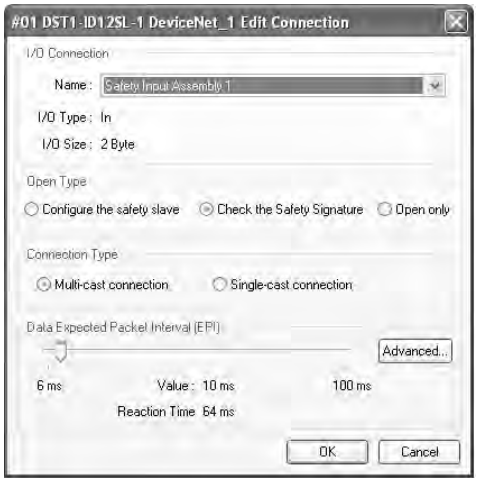
1. Set the Network Configuration Pane to display a network that has a Safety Master.
   For an NE2A-series Controller, display the NE2A Backplane to display a list of connections.
2. Select ***Edit All Connections*** from the Network Menu
   The Edit All Connections Dialog Box will be displayed.



The following table describes the information that is displayed in the Edit All Connections Dialog Box.

Item	Description
Product Name	Displays the name of the registered Safety Slave (icon) and the name of the I/O assembly used in the set Safety Connection (icon).
Open Type	Displays the open type of the I/O assembly. For details on open types, refer to *5-4-2 Setting Safety Connections*.
Con. Type	Displays the connection type of the I/O assembly. For details, refer to *5-4-2 Setting Safety Connections*.
EPI	Displays the EPI (Expected Packet Interval) of the I/O assembly. Refer to *5-4-2 Setting Safety Connections* for information on EPI.
Reaction Time	Displays the network response time of the Safety Connection.
I/O Type	Displays the type of I/O assembly used by the Safety Connection.
Size	Displays the size of the I/O assembly data used by the Safety Connection.

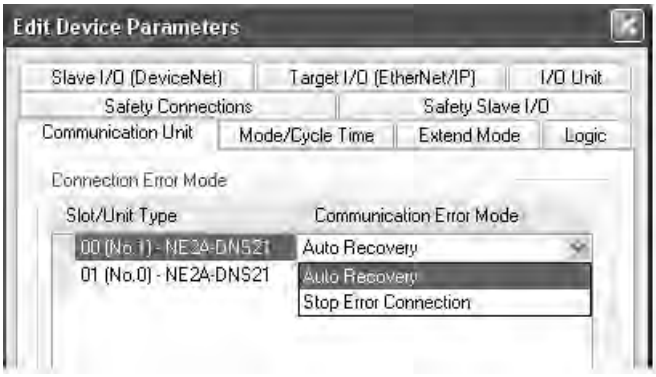
3. Select the connection for which you will change the setting and click the **Edit** Button.
   You can also double-click the connection.
   A dialog box will be displayed to register the connection.



Refer to *11-4-2 Setting Safety Connection Parameters* for information on how to use the dialog box to register the connection.

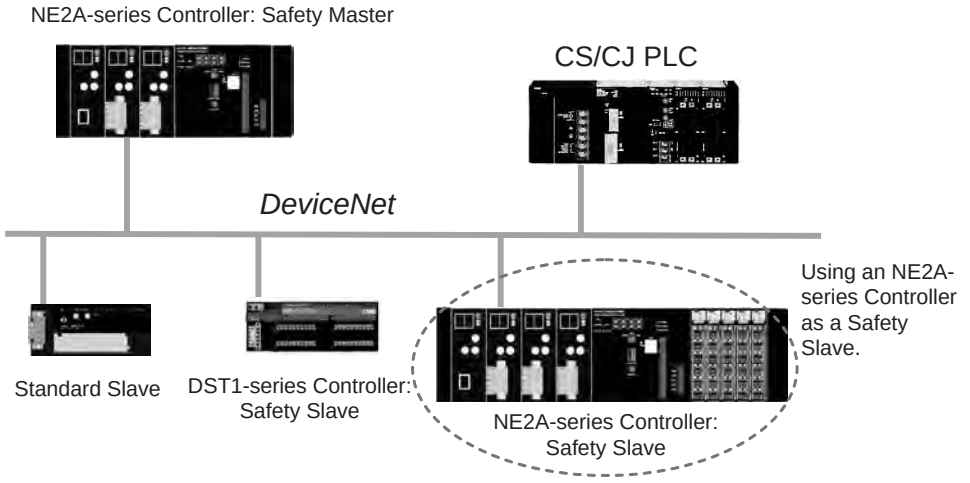
11-4-4 Stopping or Restarting Communications after an Error

With the NE2A Series, the user can specify whether to stop or continue I/O communications if a connection timeout occurs during Safety I/O Communications with a Safety Slave. If I/O communications are stopped because of a timeout error, the communications can be restarted from the Network Configurator or logic program.



11-5 Using the NE2A-series Controller as a Safety Slave

This section describes how to make settings to use an NE2A-series Controller as a Safety Slave in a DeviceNet network.
Set an I/O assembly for a Safety Slave to operate the NE2A-series Controller as a Safety Slave. The I/O assembly can be selected with an NE2A-series Controller as the Safety Master. Variables and I/O tags can be used in the Logic Editor.

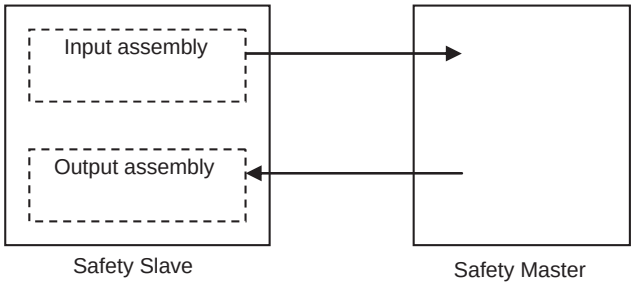


Note
(1) This setting is not required if the NE2A-series Controller is not used as a Safety Slave.
(2) An NE1A-series Controller cannot be used as a Safety Master for an NE2A-series Controller.

11-5-1 Registering I/O Assemblies for Safety Slaves

Register I/O assemblies for a Safety Slave to enable an NE2A-series Controller to function as a Safety Slave.

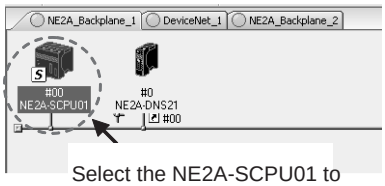
The input assembly is data from the Safety Slave to the Safety Master.
The output assembly is data from the Safety Master to the Safety Slave.



Note
(1) Up to 8 input assemblies and 8 output assemblies can be registered for a Safety Slave. (A maximum of 4 Safety Slave connections can be set for one DeviceNet Unit.)
(2) The maximum size for DeviceNet Safety I/O assemblies is different from the maximum size for EtherNet/IP Safety I/O assemblies. Take this into account when you make the connection settings.
- DeviceNet Safety Slave I/O assembly: 16 bytes max.
- EtherNet/IP Safety Slave I/O assembly: 32 bytes max.

Procedure

1,2,3... 1. Select the NE2A-SCPU to be used as a Safety Slave.

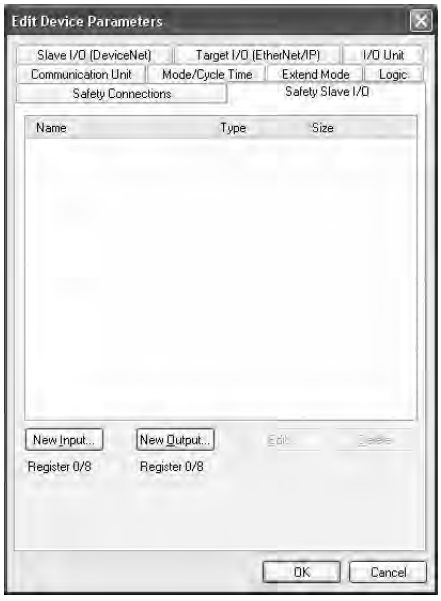


Select the NE2A-SCPU01 to be used as a Safety Slave.

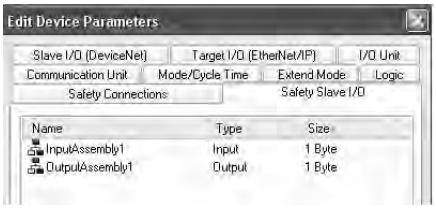
2. Select ***Parameter - Edit*** from the Device Menu.
You can also right-click the NE2A-SCPU device to be used as the Safety Slave and select ***Parameter - Edit*** from the menu.
Or, you can double-click the NE2A-SCPU device to be used as the Safety Slave.
The Edit Device Parameters Dialog Box will be displayed.



3. Click the **Safety Target I/O** Tab.
The Safety Target I/O Tab Page will be displayed in the Edit Device Parameters Dialog Box.



The following will be displayed when I/O assemblies are registered.



The following information is displayed in the Safety Slave I/O Tab Page.

Item	Information displayed
Name	The name of the registered I/O assembly (icon) is displayed.
Type	The type of input and output of the I/O assembly is displayed. • Input: Input to Slave (output assembly) • Output: Output form Slave (input assembly)
Size	The size of the I/O assembly is displayed.

Adding an Input Assembly

Procedure

1,2,3... 1. Click the **New Input** Button on the Safety Target I/O Tab Page.
The Edit Safety Target I/O Dialog Box will be displayed.



2. Make the settings for the input assembly and click the **OK** Button.
   Refer to *11-5-2 Setting Assembly Data* for information on I/O assembly data.

Note Up to 8 input assemblies and 8 output assemblies can be registered for a Safety Slave.

Adding an Output Assembly

Procedure

1,2,3...

1. Click the **New Output** Button on the Safety Target I/O Tab Page.
   The Edit Safety Target I/O Dialog Box will be displayed.
   The subsequent steps are the same as those given above in *Adding an Input Assembly.*

Changing I/O Assemblies

Procedure

1,2,3...

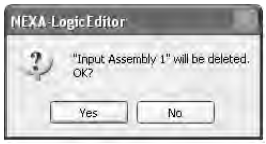
1. Select the I/O assembly to change.
2. Click the **Edit** Button on the Safety Target I/O Tab Page.
   The Edit Safety Target I/O Dialog box will be displayed.
3. Change the I/O assembly data and click the **OK** Button.
   Refer to *11-5-2 Setting Assembly Data* for information on changing I/O assembly data.

Deleting I/O Assemblies

Procedure

1,2,3...

1. Select the I/O assembly to delete.
2. Click the **Delete** Button on the Safety Target I/O Tab Page.
   A dialog box to confirm the deletion will be displayed.

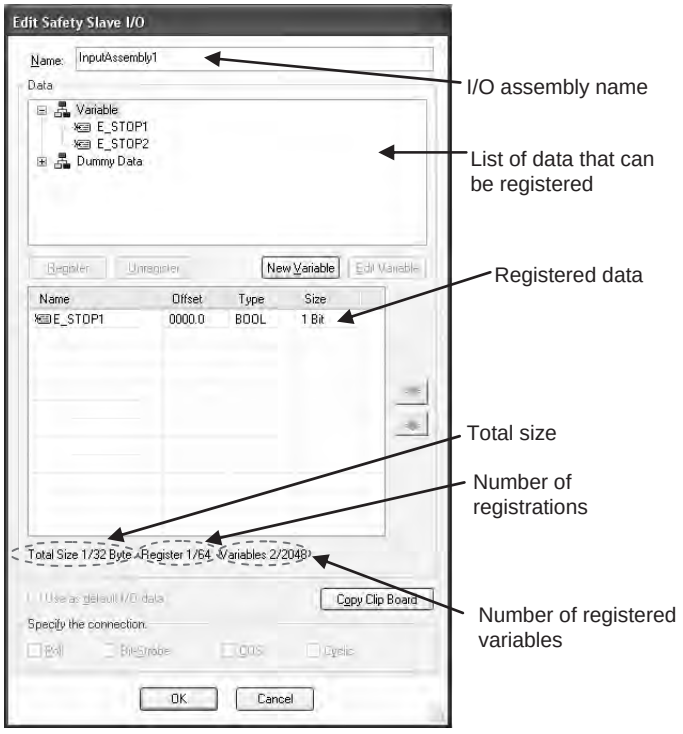


3. Click the **OK** Button.
   The I/O assembly will be deleted.

11-5-2 Setting Assembly Data

This section describes how to define data for I/O assemblies.

Edit Safety Target I/O Dialog Box



I/O Assembly Name

The I/O assembly name can be edited.

Note An I/O assembly name can contain up to 48 characters.
The characters that can be input are the same as those that can be input for variables. Refer to *Variable Specifications* on page 80.

List of Data That Can Be Registered

This list displays the data that can be registered to I/O assemblies.
For details, refer to *5-8-2 Configuring Assemblies*.

New variables can be created and registered. For details, refer to *Creating New Variables* on page 265, below.

Note Dummy data is used if the Master can transfer only an even number of bytes. Dummy data cannot be registered at the start.

Registered data List

This list displays data that was registered from the list of data that can be registered. The following information is displayed in the registered data List.

Item	Information displayed
Name	The name of the registered data is displayed.
Offset	The position in I/O assembly data of allocated data is displayed.
Type	The type of the registered data is displayed.
Size	The size of the registered data is displayed.

Total Size

This area displays the total size of the I/O assembly. A maximum of 32 bytes can be registered for one input assembly and 32 bytes for one output assembly.

An I/O assembly of up to 32 bytes can be set for an EtherNet/IP Safety configuration, but the maximum for an I/O assembly in a DeviceNet Safety configuration is 16 bytes.

Note The data size will be set as one byte if the data size is less than one byte, e.g., for BOOL variables and local I/O input data.

Number of Registrations

The number of data items registered to the I/O assembly is displayed here. A maximum of 64 status information items can be registered for one input assembly and 64 for one output assembly.

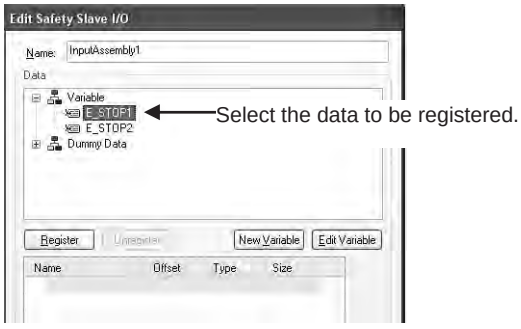
Number of Registered Variables

The total number of input and output variables that has been registered is displayed. Up to 2,048 variables can be registered total for input and output variables.

Registering Data

Procedure

1,2,3... 1. Select the data to be registered from the list of data that can be registered.



2. Click the **Register** Button.
The data will be displayed in the list of registered data.



The total size and the number of registrations will be updated.

Unregistering Data

Procedure

1,2,3... 1. Select the data for which the registration is to be deleted from the list of register data.



2. Click the **Unregister** Button.
The data will be unregistered and deleted from the list of registered data.



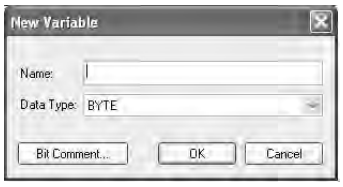
The total size and the number of registrations will be updated.

Creating New Variables

It is possible to create variables to allocate to I/O assemblies in the Edit Safety Target I/O Dialog Box.
Variables to allocate to I/O assembles can also be created in the Logic Editor. Refer to *15-5 Creating Variables* for information on the procedure for creating these variables in the Logic Editor.

Procedure

1,2,3... 1. Click the **New Variable** Button in the Edit Safety Target I/O Dialog Box.
The New Variable Dialog Box will be displayed.

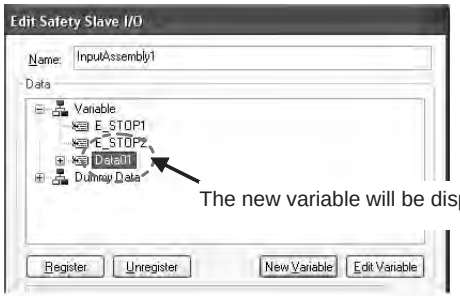


2. Set the variable data and click the **OK** Button.
The following table describes the settings in the New Variable Dialog Box.

Setting	Description
Name	Specifies the variable name. Up to 48 characters (48 bytes max.) can be used. Names are not case sensitive if ASCII alphanumeric characters are used. The following characters cannot be used: : ! # $ % & ' " ( ) = ~ ^ \ | ` @ { + ; * : } < , > ? / . [ ] Also the following cannot be used: • The first character cannot be a number. • Reserved characters cannot be used.
Data type	Select from BOOL, BYTE, WORD, or DWORD.

The Edit Bit Comment button will be enabled if BOOL is not selected for the data type. (For details, refer to *Editing Bit Comments* on page 266 in the following section.)

A new variable will be added to the list of data that can be registered in the Edit Safety Target I/O Dialog Box.



Editing Bit Comments

1,2,3... 1. Click the **Edit Bit Comment** Button.
The Edit Bit Comment Dialog Box will be displayed.



2. Enter a comment for each bit and press the **Enter** Key.
3. Click the **OK** Button. The bit comment will be set.

Note Up to 48 characters (48 bytes) can used for the bit comment.
The characters that can be input are the same as those that can be input for variables. Refer to *Variable Specifications* on page 80.

Editing

You can edit registered variables. For information on the procedure, refer to *Creating New Variables* on page 265 above.

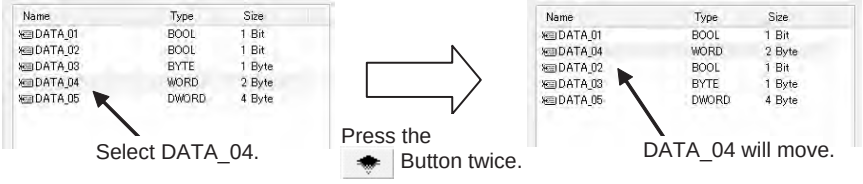
Changing the Order of Registered Data

You can change the order of registered data.

Procedure

1,2,3...

1. Select the registered data that you will change the order of.
2. Click the  Button (move up) or  Button (move down).
The registered data that is selected will move.
Example:



Note BOOL data can be arranged in BYTE, WORD, or DWORD data. If longer variables, such as BYTE variables, are placed between continuous BOOL variables, the total data size will change.

11-5-3 Registering I/O Assemblies from the Logic Editor

You can register I/O assemblies from the Logic Editor.

Procedure

1,2,3...

1. Select ***Setting - Target I/O*** from the Device Menu of the Logic Editor.
The Target/Slave I/O Settings Dialog Box will be displayed.
2. Click the **Safety Target I/O** Tab.



3. Click the **New Input** Button (or **New Output** Button). The Edit Safety Target I/O Dialog Box will be displayed.

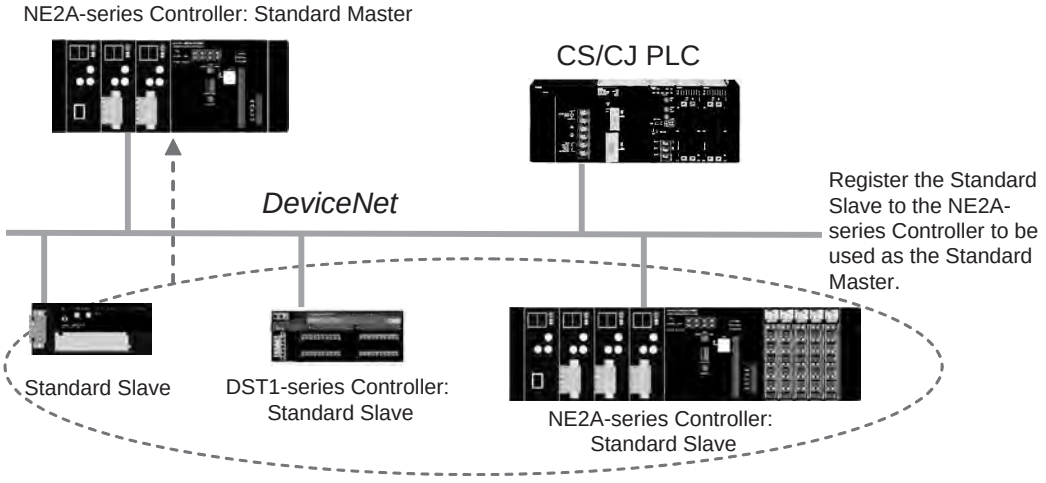
The procedures for adding, changing, and deleting I/O assemblies are the same as the procedures using the Network Configurator. For details, refer to *11-5-1 Registering I/O Assemblies for Safety Slaves*.

11-6 Communications between the NE2A-series Controller and Standard Slaves

This section describes how to make settings to use an NE2A-series Controller as a Standard Master in a DeviceNet network. To operate an NE2A-series Controller as a Standard Master, register the device that will be the Standard Slave and set the connection.

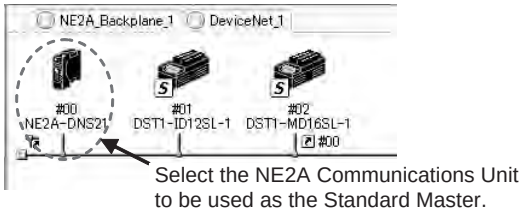
11-6-1 Registering Standard Slaves

Register the Standard Slave to communicate with and set the connection. Refer to *11-3 DeviceNet Network Settings* for information on building DeviceNet networks.
This section describes how to set a Standard Connection with a DeviceNet network that is already built. Refer to *5-5-2 Standard Connection Settings* for information on Standard Connections.

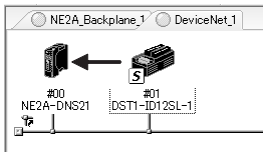


Procedure

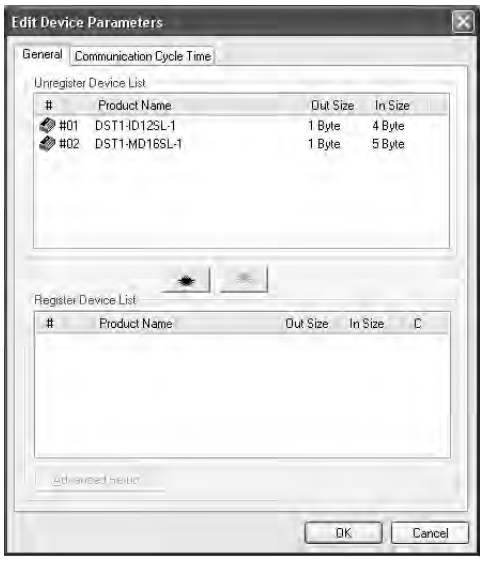
1,2,3... 1. Select the NE2A-DNS21 of the NE2A-SCPU01 for which Master settings will be performed.



Steps 4 and 5 can be eliminated by dragging and dropping the Standard Slave to the NE2A-series NE2A-DNS21 to be used as a Standard Master in the Network Configuration Pane.



2. Select ***Parameter - Edit*** from the Device menu.
   You can also right-click the device to set as a Standard Master, and then select ***Parameter - Edit*** from the menu.
   Or, you can double-click the Master to be set.
   The Edit Device Parameters Dialog Box will be displayed.
3. Click the **General** Tab.
   All devices registered in the same network will be displayed in the Unregister Device List Area (except local devices).



The following information is displayed in the list of unregistered devices.

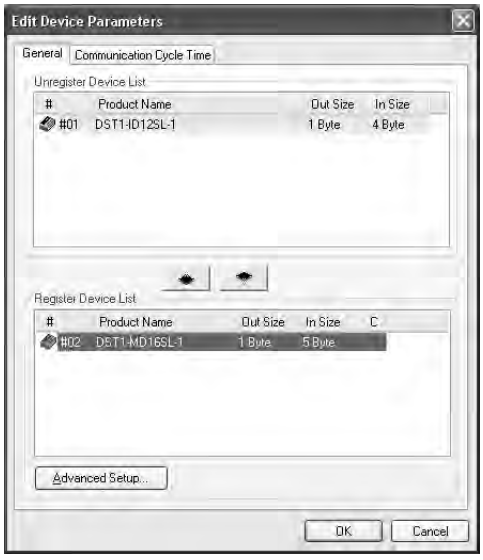
Item	Description
#	The node address of the device is displayed.
Product Name	A description of the device is displayed.
Out Size	The total size of the output assembly is displayed.
In Size	The total size of the input assembly is displayed.

The following information is displayed in the list of registered devices.

Item	Description
#	The node address of the device is displayed.
Product Name	A description of the device is displayed.
Out Size	The total size of the output assembly is displayed.
In Size	The total size of the input assembly is displayed.
C	Whether there are detailed connection settings is displayed. *: Detailed settings

4. Select the Slave for which the connection will be set from the Unregister Device List Area.

5. Click the  Button.
   The Slave will be registered and displayed in the Register Device List Area.

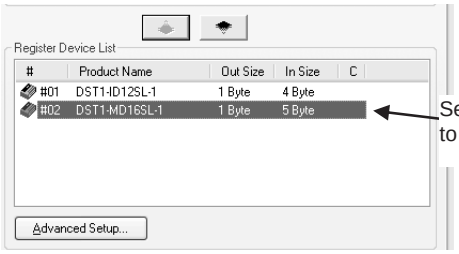


The default I/O assembly will be registered if the *Auto allocation as is registered* Option is selected.

Unregistering Slave Devices

Procedure

1,2,3... 1. Select the Slave to be unregistered in the Register Device List on the General Tab Page.

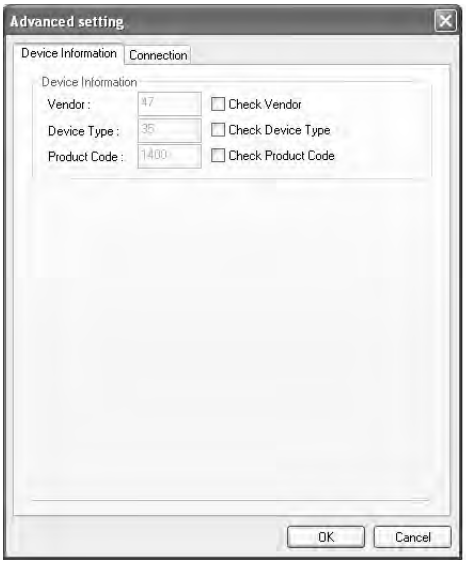


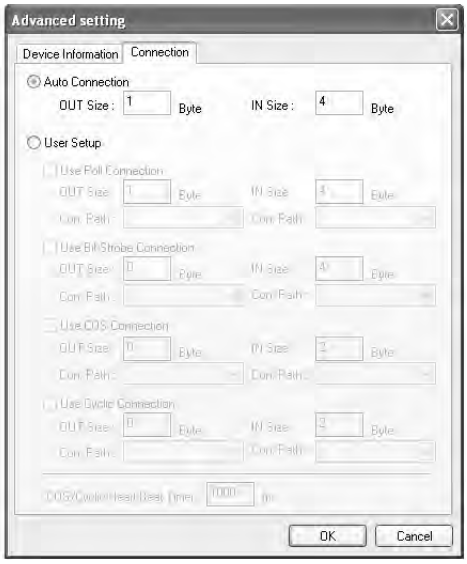
2. Click the  Button.
The Slave will be unregistered and removed from the Register Device List.

11-6-2 Setting Standard Connections

This section describes how to set parameters for a Standard Connection.

Click the **Advanced Setup** Button in the Edit Device Parameters Dialog Box to make the settings in the following Advanced setting Dialog Box.





Device Information

Use the Device Information Tab Page to verify device information when the Standard Master is online to the network with the actually connected Slaves.
For details, refer to *5-5-2 Standard Connection Settings*.

Connection Information

Automatic Connection Setting

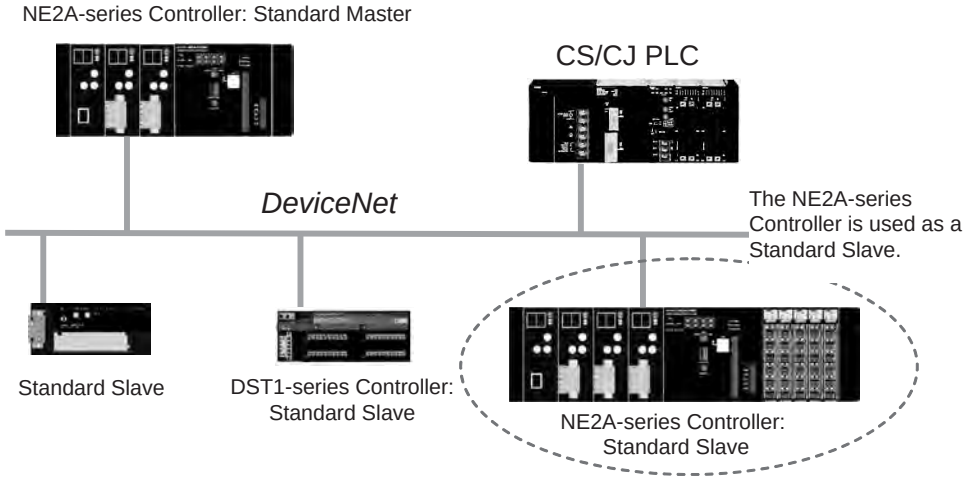
Specify the default connection set for the Standard Slave. With the NE2A-series Controller, an assembly will be applied if the Use as default I/O Option is selected when an assembly for a Standard Slave is created.

Manual Connection Setting

Select the type of connection to use between the NE2A-series Controller and the Standard Slave.
For details, refer to *5-5-2 Standard Connection Settings*.

11-7 Using an NE2A-series Controller as a Standard Slave

The NE2A-series Controller can be used as a Standard Slave. To operate an NE2A-series Controller as a Standard Slave, set an I/O assembly for a Standard Slave. The I/O assembly can be selected with an NE2A-series Controller or other Controller as the Standard Master.

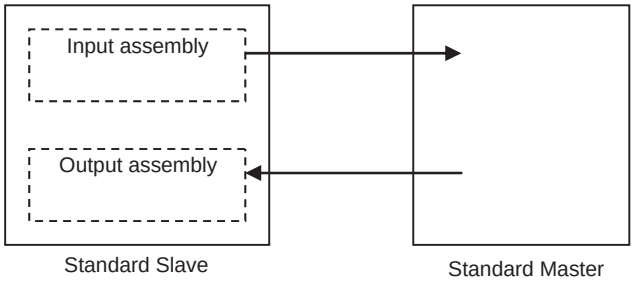


Note This setting is not required if the NE2A-series Controller will not be used as a Standard Slave.

11-7-1 Registering I/O Assemblies for Standard Slaves

Register I/O assemblies for a Standard Slave to enable an NE2A-series Controller to function as a Standard Slave.

The input assembly is data from the Standard Slave to the Standard Master.
The output assembly is data from the Standard Master to the Standard Slave.

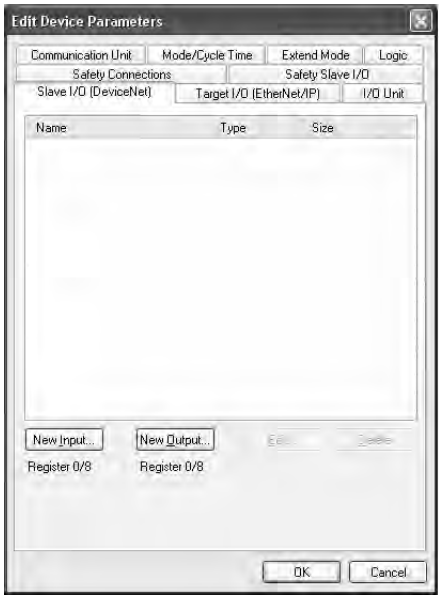


Note Up to 8 input assemblies and 8 output assemblies can be registered for a Standard Slave.

Procedure

1,2,3...

1. Select the NE2A-SCPU01 to be used as a Standard Slave.
2. Select ***Parameter - Edit*** from the Device Menu.
   You can also right-click the NE2A-SCPU01 device and select ***Parameter - Edit*** from the menu.
   Or, you can double-click the NE2A-SCPU01.
   The Edit Device Parameters Dialog Box will be displayed.
3. Click the **Slave I/O (DeviceNet)** Tab.
   The Slave I/O (DeviceNet) Tab Page on the Edit Device Parameters Dialog Box will be displayed.



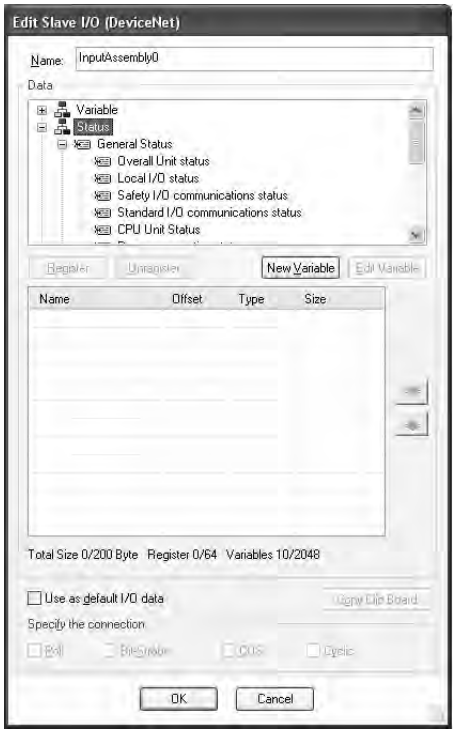
The following information is displayed on the Slave I/O (DeviceNet) Tab Page.

Item	Information displayed
Name	The name of the registered I/O assembly ( ) and the name of the I/O tag defined in the assembly ( ) are displayed.
Type	The type of I/O assembly (i.e., input or output) and the data type of the I/O tag are displayed.
Size	The size of the I/O assembly and the size of each I/O tag are displayed.

Adding an Input Assemble

Procedure

1,2,3... 1. Click the **New Input** Button on the Slave I/O (DeviceNet) Tab Page. The Edit Slave I/O (DeviceNet) Dialog Box will be displayed.



2. Set the data for the input assembly and click the **OK** Button.
   Refer to *11-7-2 Setting Assembly Data* to set the I/O assembly data.

Adding an Output Assembly

Procedure

1,2,3...

1. Click the **New Output** Button on the Slave I/O (DeviceNet) Tab Page.
   The Edit Slave I/O (DeviceNet) Dialog Box will be displayed.
   The subsequent steps are the same as those given above in *Adding an Input Assembly*.

Changing I/O Assemblies

Procedure

1,2,3...

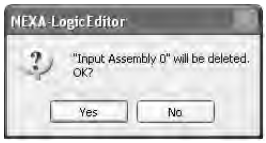
1. Select the I/O assembly to be changed.
2. Click the **Edit** Button on the Slave I/O (DeviceNet) Tab Page.
   The Edit Slave I/O (DeviceNet) Dialog Box will be displayed.
3. Change the I/O assembly data and click the **OK** Button.
   Refer to *11-7-2 Setting Assembly Data* to set the I/O assembly data.

Deleting I/O Assemblies

Procedure

1,2,3...

1. Select the I/O assembly to be deleted.
2. Click the **Delete** Button on the Slave I/O (DeviceNet) Tab Page.
   A dialog box will be displayed to confirm the deletion.

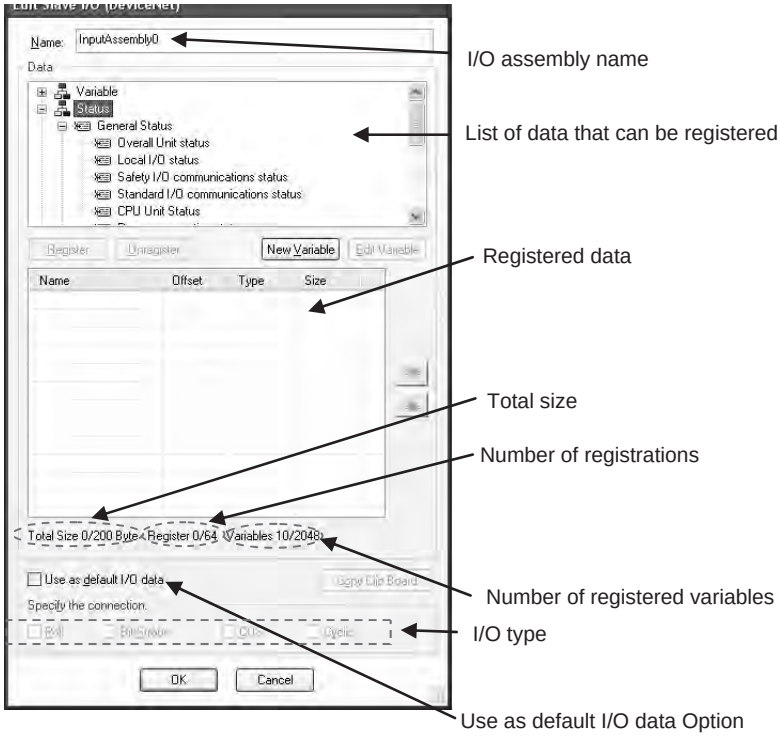


3. Click the **Yes** Button.
   The Standard Slave I/O will be deleted.

11-7-2 Setting Assembly Data

This section describes how to define data for I/O assemblies.

Edit Slave I/O (DeviceNet) Dialog Box



Refer to *11-5-2 Setting Assembly Data* for information on the following items.

- ✧ **I/O assembly names**
- ✧ **List of data that can be registered**
- ✧ **List of registered data**

Total Size

This area displays the total size of the I/O assembly. A maximum of 200 bytes can be registered for one input assembly and 200 bytes for one output assembly.

Note The data size will be set as one byte if the data size is less than one byte, e.g., for BOOL variables and local I/O input data.

Number of Registrations

The number of data items registered to the I/O assembly is displayed here. A maximum of 64 status information items can be registered for one input assembly and 64 for one output assembly.

Number of Registered Variables

The total number of input and output variables that has been registered is displayed. Up to 2,048 variables can be registered total for input and output variables.

Use as Default I/O Data Option

Use this option to specify the default connection. Connections of I/O assemblies for which this option is selected will be automatically registered when automatic allocation is used and registration is performed with the Master.
If this option is selected for an I/O assembly, the selection will be cleared for the I/O assembly for which it was previously selected.

I/O Type

Use this property to select the type of connection for I/O communications in DeviceNet Standard Communications. Refer to *5-5-2 Standard Connection Settings* for information on connection types.

The I/O type cannot be set for output assemblies.

Registering, Unregistering, Creating, and Editing Data

Refer to *11-5-2 Setting Assembly Data* for information on registering, unregistering, creating, and editing data.

11-7-3 Registering from the Logic Editor

You can register I/O assembles from the Logic Editor.

Procedure

1,2,3...

1. Select ***Settings - Target I/O*** from the Device Menu of the Logic Editor. The Target/Slave I/O Settings Dialog Box will be displayed.
2. Click the **Slave I/O (DeviceNet)** Tab.
   The Slave I/O (DeviceNet) Tab will be displayed in the Target/Slave I/O Settings Dialog Box.
3. Click the **New Input** Button or **New Output** Button. The Edit Slave I/O Dialog Box will be displayed.

The procedures for adding, changing, and deleting I/O assemblies are the same as the procedures in *11-7-1 Registering I/O Assemblies for Standard Slaves*.

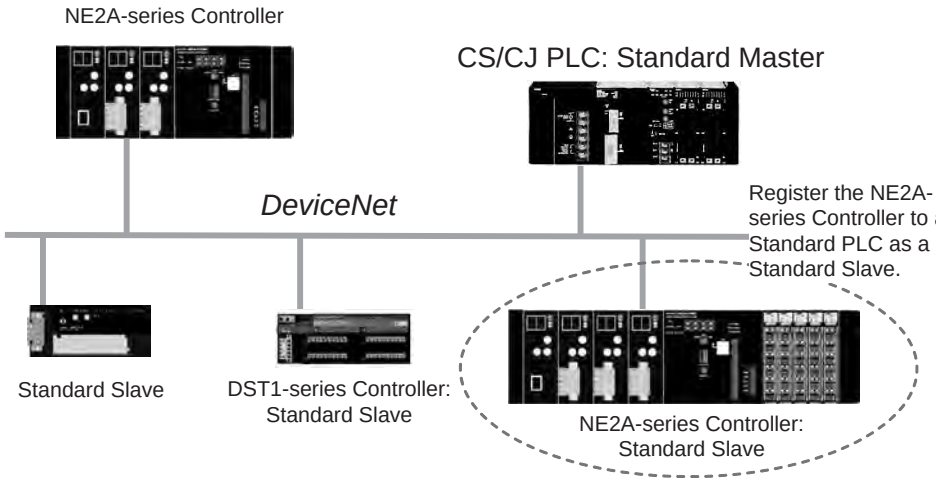
11-7-4 Setting Slave Input Data in IDLE Mode

You can set to hold or clear the previous data in any of the following cases for input assembles transferred from an NE2A-series Standard Slave to a Standard Master.

- The NE2A-series Controller is changed from RUN Mode to IDLE Mode.
- A communications error or other error is detected in a safety chain that sets data to I/O tags of input assemblies.

11-8 Communications between an NE2A-series Controller and a Standard Master

This section describes how to makes settings to perform communications with a Standard Master device, such as a Standard PLC) with an NE2A-series Controller used as a Standard Slave.

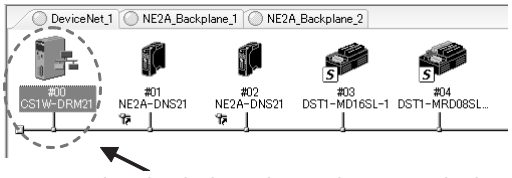


Registering DeviceNet Units (Standard Slaves)

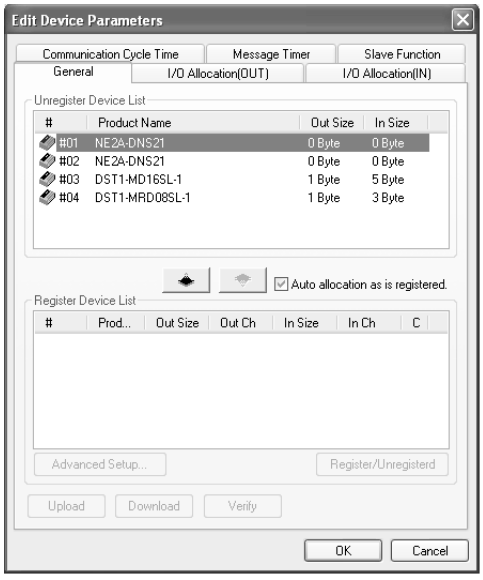
Use the following procedure to register an NE2A-series DeviceNet Unit (NE2A-DNS21) that is set as a Standard Slave on a DeviceNet network to the device to be used as a Standard Master.

Procedure

1,2,3... 1. Select the device to be used as a Standard Master.

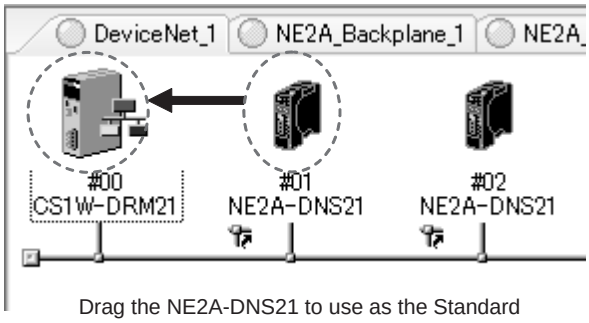


2. Select ***Parameter - Edit*** from the Device Menu.
   You can also right-click the selected device and select ***Parameter - Edit*** from the menu.
   Or, you can double-click the device.
   The Edit Device Parameters Dialog Box will be displayed.



3. Select the NE2A-DNS21 to use as a Standard Slave and click the  Button.
   The NE2A-DNS21 will be registered to the device to be used as the Standard Master.

   Step 3 can be eliminated by dragging and dropping the NE2A-series NE2A-DNS21 to use as a Standard Slave to the Standard Master in the Network Configuration Pane.



Drag the NE2A-DNS21 to use as the Standard Slave to the CS1W-DRM21 to use as the Standard Master.

Refer to the manual of the relevant DeviceNet device for information on setting devices as Standard Masters.

SECTION 12
Setting EtherNet/IP Networks

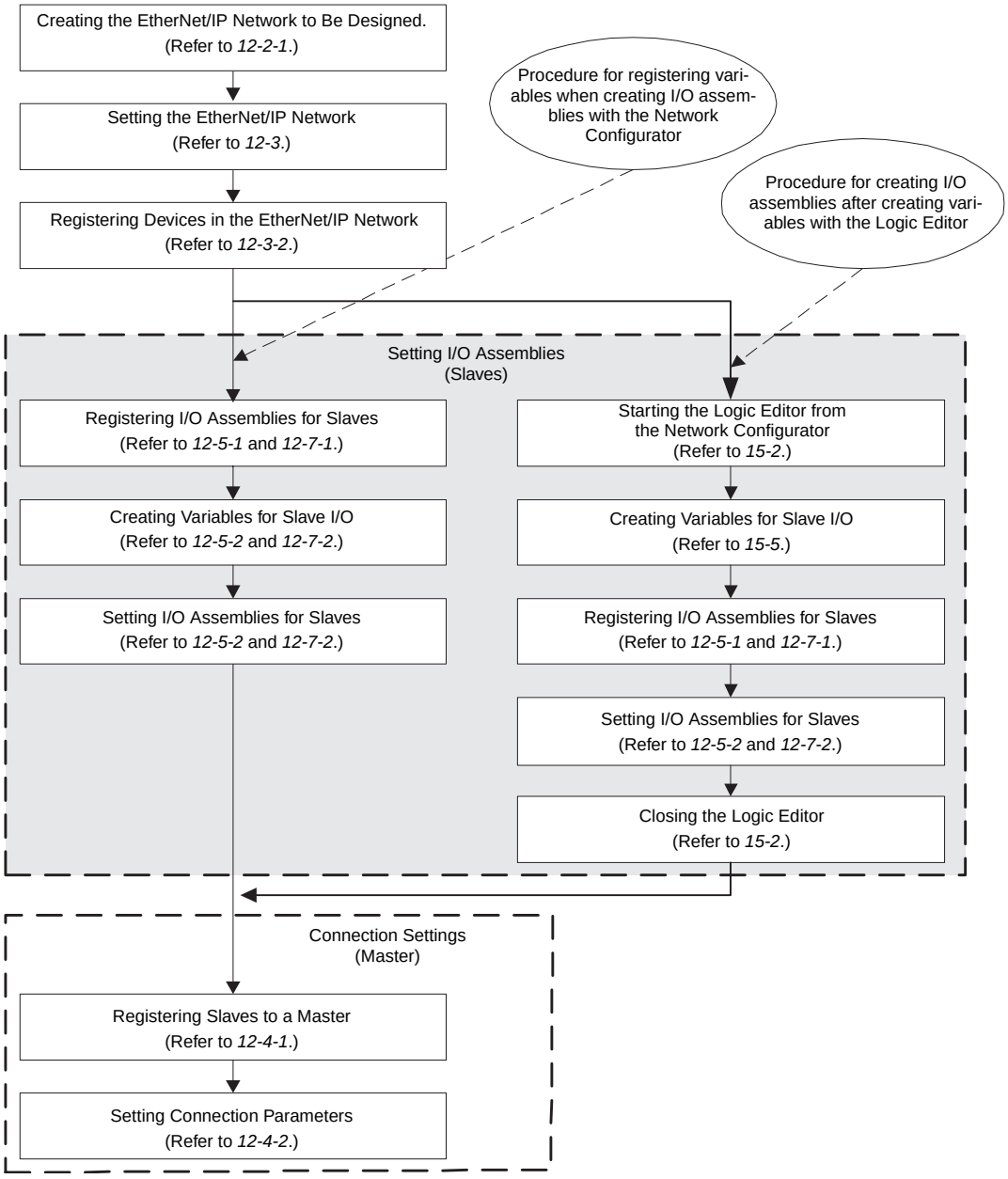
This section describes how to set up EtherNet/IP networks for a NE2A-series Safety Network Controller.

12-1 EtherNet/IP Network Setting Procedure 282
12-2 Registering EtherNet/IP Units to the CPU Unit 283
12-2-1 Associating the CPU Unit and EtherNet/IP Units 283
12-3 EtherNet/IP Network Settings 286
12-3-1 Setting IP Addresses 286
12-3-2 Adding Devices to a Network 289
12-3-3 TCP/IP Settings 291
12-4 Communications between an NE2A-series Controller and a Safety Slave . . . 292
12-4-1 Registering Safety Slaves 292
12-4-2 Setting Safety Connection Parameters 294
12-4-3 Convenient Functions for Editing Connections 295
12-4-4 Stopping or Restarting Communications after an Error 295
12-5 Using the NE2A-series Controller as a Safety Slave 296
12-5-1 Registering I/O Assemblies for Safety Slaves 296
12-5-2 Setting Assembly Data 296
12-5-3 Registering I/O Assembles from the Logic Editor 296
12-6 Communications between the NE2A-series Controller and Standard Slaves . 297
12-7 Using an NE2A-series Controller as a Standard Slave 298
12-7-1 Registering I/O Assemblies for Target Devices 298
12-7-2 Setting I/O Assemblies 300
12-7-3 Registering I/O Assemblies from the Logic Editor 305
12-7-4 Setting Slave Input Data in IDLE Mode 306

12-1 EtherNet/IP Network Setting Procedure

This section describes how to build and set an EtherNet/IP network to perform EtherNet/IP communications. With NE2A-series Controllers, any of the following functions can be set for each EtherNet/IP Unit: Safety Master, Safety Slave, or Tag Data Links (Target).

The Slave procedure is not required if the NE2A-series Controller will not be used as a Safety Slave or used in Tag Data Links (Target).



12-2 Registering EtherNet/IP Units to the CPU Unit

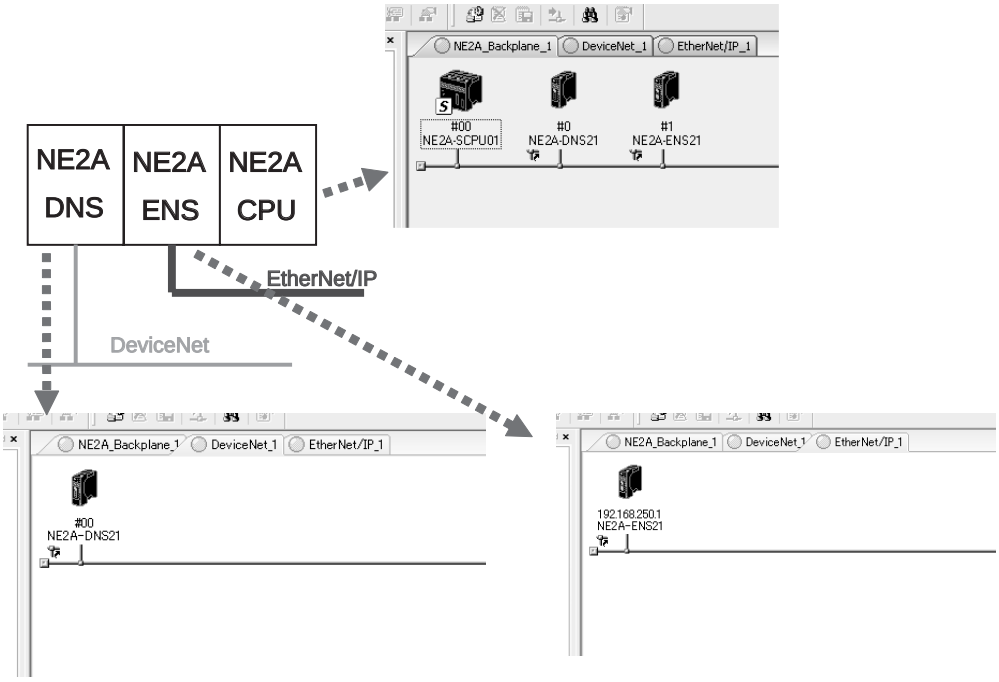
This section describes the procedure for registering EtherNet/IP Units to an NE2A-series CPU Units to build an EtherNet/IP network.

12-2-1 Associating the CPU Unit and EtherNet/IP Units

An NE2A-series CPU Unit does not have a communications port for DeviceNet or EtherNet/IP communications. To perform DeviceNet or EtherNet/IP communications, mount an NE2A-DNS21 DeviceNet Unit or an NE2A-ENS21 EtherNet/IP.

To associate these Communications Units with a CPU Unit, register them to the NE2A-series Backplane of the CPU Unit.

The following figure shows display examples of the Unit configuration in the Network Configurator.

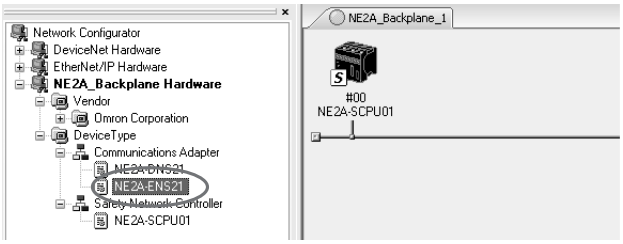


Registering EtherNet/IP Units

Register the NE2A-ENS21 EtherNet/IP Unit to the NE2A-series Backplane.

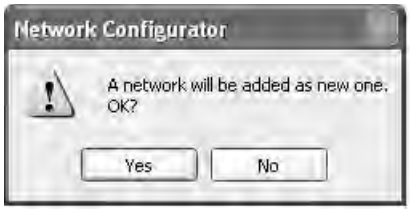
Procedure

1,2,3... 1. Double-click *NE2A-ENS21* in the Hardware List Pane. You can also drag *NE2A-ENS21* from the Hardware List Pane and drop it in the Network Configuration Pane.

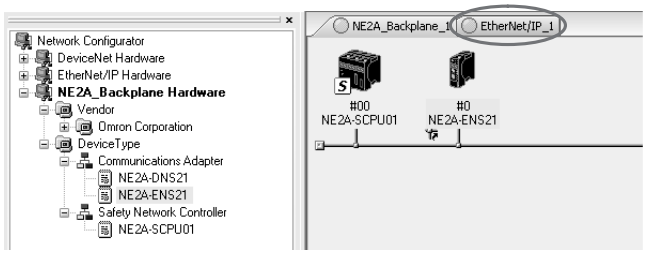


2. Select the NE2A-ENS21 added in step 1.

3. Select ***Register to Routing Network*** from the Device Menu.
   You can also right-click the NE2A-ENS21 and select ***Register to Routing Network*** from the menu.
   A dialog box will be displayed to confirm whether to add to the network.



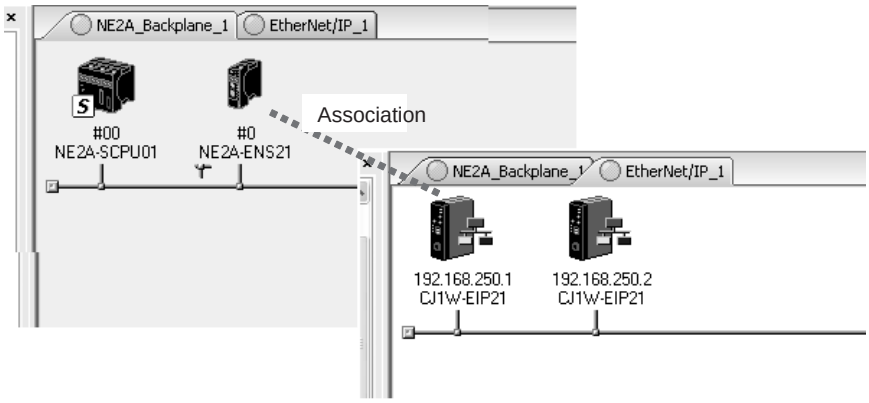
4. Click the **OK** button.
   An EtherNet/IP Tab will be added to the Network Configuration Pane.



Note The slot numbers of the device parameters will be assigned in the order that the Communications Unit is added to the NE2A Backplane. Change the slot number to match the actual configuration by using the tab page for the Communications Unit in the Edit Device Parameters Dialog Box. This dialog box is displayed by selecting ***Parameter - Edit*** from the Device Menu. (Refer to *11-2-1 Associating the CPU Unit and DeviceNet Units*.)

Associating an NE2A-series Backplane with Other Networks

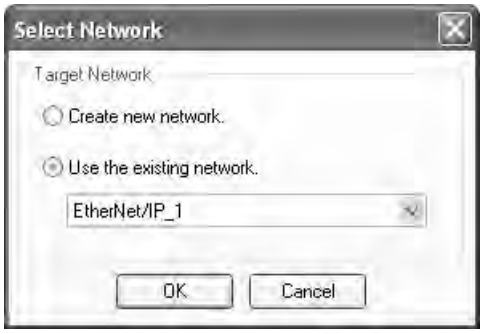
Associations can be made to the NE2A-series Backplane after creating the EtherNet/IP network.



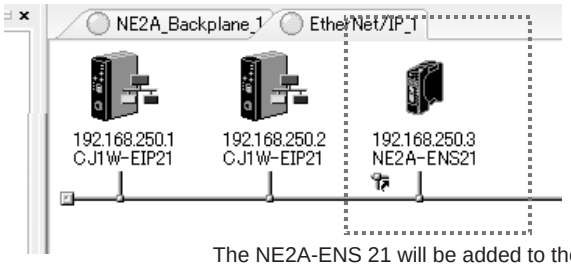
Procedure

1,2,3...

1. Add a NE2A-ENS21 to the NE2A-series Backplane of the NE2A-series Controller.
2. Select the NE2A-ENS21.
3. Select ***Register to Routing Network*** from the Device Menu.
   You can also right-click the NE2A-ENS21 and select ***Register to Routing Network*** from the menu.
   The Select Network Dialog Box will be displayed.



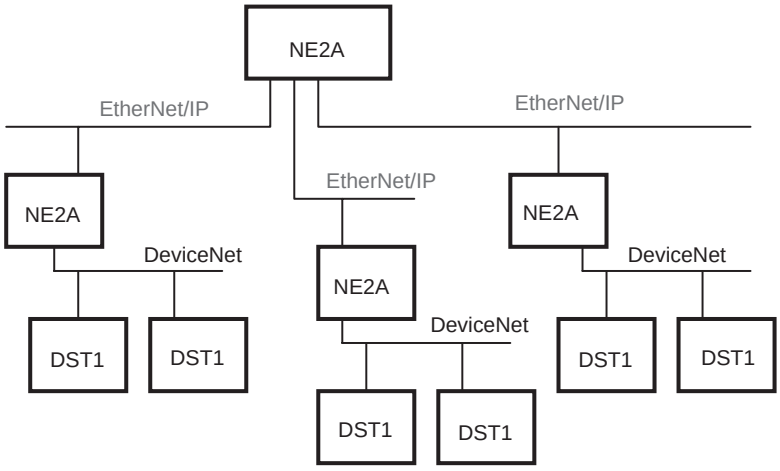
4. Select the *Use the existing network* Option and select the network name to be associated.
5. Click the **OK** Button.
   The network associations will be made.



The NE2A-ENS 21 will be added to the network.

12-3 EtherNet/IP Network Settings

More than one Communications Unit can be connected in an NE2A-series Controller, so it is often necessary to manage multiple networks. This section describes how to make TCP/IP settings to manage EtherNet/IP networks.



12-3-1 Setting IP Addresses

IP addresses that consist of a network ID and host ID are used on an Ethernet network to uniquely identify devices and perform mutual confirmation. For details, refer to *5-2-3 EtherNet/IP Communications*.

Any of the following methods can be used to set the IP address for an EtherNet/IP Unit.

- Set the IP address with the IP address setting switches.
- Set the IP address from the Network Configurator.
- Set the IP address using BOOTP.

If an IP address is changed, an error for incorrect operation of the rotary switches after startup will occur in the EtherNet/IP Unit and "C8" will be displayed on the 7-segment display. You must perform the procedure to change the IP address in the configuration data given in *Changing Device Addresses* on page 289 and download settings so that the IP address setting on the EtherNet/IP Unit and the IP address in the configuration data are the same.

Setting the IP Address with the IP Address Setting Switches

If the IP address setting switches are set to 01 to FE, the EtherNet/IP Unit creates the IP address using the network ID set from the Network Configurator and the IP address setting switches.

If the network ID has not been set from the Network Configurator, operation will be performed with the default ID (192.168.250). The following IP address will thus be used be used.

IP address = 192.168.250.*Host ID set on IP address setting switches*

To change the network ID, refer to *Setting the IP Address from the Network Configurator* in the next section.

Setting the IP Address from the Network Configurator

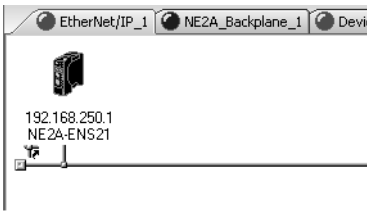
Set the IP address from the TCP/IP Settings Dialog Box of the Network Configurator with the Network Configurator connected online.

Procedure

1,2,3... 1. Set the IP address setting switches on the EtherNet Unit to the host ID of the IP address to be set.

IP address = Network ID (default: 192.168.250) + Host ID

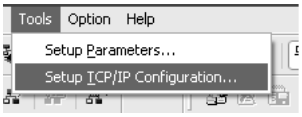
2. Display the EtherNet/IP Tab Page in the Network Configuration Pane, and select the EtherNet/IP Unit to be set.



3. Select ***Reset*** from the Device Menu.

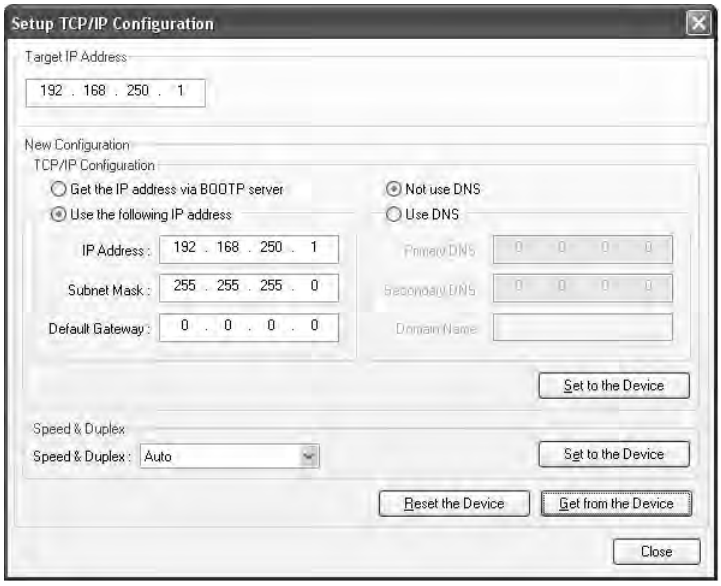


4. Select the *Return to the out-of -box configuration* Option, and then click the **OK** Button.
5. Select ***Setup TCP/IP Configuration*** from the Tools Menu.



IMPORTANT The *Setup TCP/IP Configuration* command will be displayed if the Tool Menu is selected from the EtherNet/IP Tab Page in the Network Configuration Pane.

The TCP/IP Settings Dialog Box will be displayed.



6. Set the present IP address of the EtherNet/IP Unit in the *Target IP Address* Field.

   IP address = 192.168.250.*Host ID set on IP address setting switches*

7. Select the *Use the following IP address* Option, and then set the new IP address, subnet mask, and default gateway. Set the host ID to the value set on the IP address setting switches.
8. Click the **Set to the Device** Button in the New Configuration Area to download the settings to the EtherNet/IP Unit.

Note

(1) If the node address (IP address) is not set correctly, a connection may be made with an unintended device, and incorrect device parameters may be set. Therefore, check the connection destination device before downloading the settings.

(2) NE2A-series Controllers do not support DNS. Always select *Do not use DNS* in the TCP/IP settings.

9. If a new IP address is set, the EtherNet/IP Unit will be restarted and the set IP address will be enabled as long as Safety I/O is not currently operating.

Note If Safety I/O is operating, confirm system safety and then restart the Unit.

Setting the IP Address Using BOOTP

With the EtherNet/IP Unit, the IP address can be obtained by using BOOTP. To set the IP address using BOOTP, a BOOTP server must be installed on the network.

Obtaining a BOOTP Server to Operate on a Personal Computer

The Rockwell Interactive BOOTP/DHCP Utility is recommended by ODVA as the BOOTP server. It is available from the following website: http://www.ab.com/networks/bootp.html

IMPORTANT You can access the MAC address of the EtherNet/IP Unit by using the monitor function of the EtherNet/IP Unit. (Refer to *18-4-3 Ethernet Information Tab Page*.)

Procedure

Start the BOOTP server using a personal computer connected to the Ethernet.

Set the MAC address and the IP address of the EtherNet/IP Unit to be set in the BOOTP server.

1,2,3...

1. Set the IP address setting switches on the EtherNet/IP Unit to 00.
2. Set the present IP address of the EtherNet/IP Unit in the *Target IP Address* Field in the TCP/IP Settings Dialog Box of the Network Configurator. (Refer to the previous page.)
3. Select the *Get the IP address via BOOTP server* Option.
4. Click the **Set to the Device** Button in the *New Configuration* Area, and then download the settings to the EtherNet/IP Unit.
5. Click the **Reset the Device** Button to restart the EtherNet/IP Unit. The IP address obtained using BOOTP will be displayed on the 7-segment display of the EtherNet/IP Unit.
6. Change the Target IP Address Area in the TCP/IP Settings Dialog Box to the IP address obtained from the BOOTP server, and then select the *Use the following IP address* Option. Set the obtained IP address, subnet mask, and default gateway.

7. Click the **Set to the Device** Button in the *New Configuration* Area, to download the settings to the EtherNet/IP Unit.

   From the next startup, obtaining the IP address using BOOTP will be disabled.

IMPORTANT It is possible to obtain the IP address using a BOOTP server even if the IP address setting switches are set to FF. If the setting is FF, BOOTP will be performed at every startup. Therefore, set the IP address setting switches to 00 after the IP address has been obtained, and then perform steps 6 and 7 described above.

12-3-2 Adding Devices to a Network

There are three ways to add devices to a virtual network.

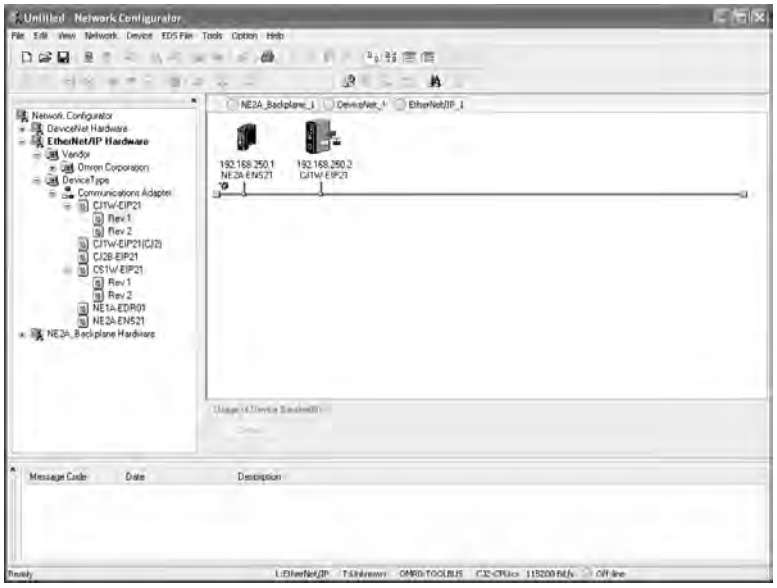
- Adding a device from the Hardware List Pane (Refer to *Adding Devices from the Hardware List*, below.)
- Obtaining the network configuration from the actual network (Refer to *17-3-2 Uploading Device Parameters*.)
- Selecting ***Add to Network*** from the EDS File Menu

Adding Devices from the Hardware List

Use the following procedure to add a device from the Hardware List Pane to the virtual network.

Procedure

1,2,3... 1. Double-click the device in the Hardware List Pane and drag it to the Network Configuration Pane.
The following display will appear when the device is registered.



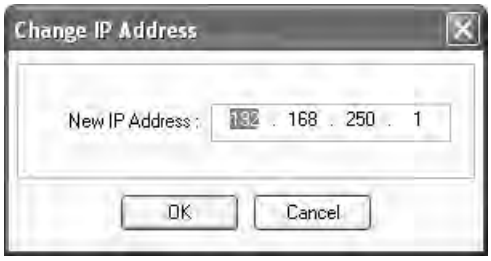
Changing Device Addresses

When a device is added to a virtual network, an unused IP address between 192.168.250.1 and 192.168.250.254 will be automatically allocated to the device. The IP address displayed on the Network Configurator will be used as the IP address in the configuration data. It must be the same as the actual IP address of the EtherNet/IP Unit. Use the following procedure to change the IP address in the configuration data.

Procedure

1,2,3... 1. Select the device for which the IP address will be changed.

2. Select the device and select ***Change IP Address*** from the Device Menu.
You can also right-click the device and select ***Change IP Address***.
The Change IP Address Dialog Box will be displayed.



3. Change the IP address and click the **OK** Button.
Set the same IP address that is set on the setting switches.
An error message will be displayed if an attempt is made to set an IP address that is being used by another device.



Note (1) Set the IP address for the device according to *12-3-3 TCP/IP Settings*.

(2) If the IP addresses of the EtherNet/IP Units have been changed from the Network Configurator, connect each Unit and download the IP address parameters for the TCP/IP settings.

Changing the Device Name

You can change the name of a device. When you add a device from the Device List, the name that is displayed will be the name from the Device List.

Procedure

1,2,3... 1. Select the device for which the device name will be changed.

2. Select ***Change Device Comment*** from the Device Menu.
You can also right-click the device and select ***Change Device Comment***.
The Change Device Comment Dialog Box will be displayed.



3. Enter a device name and click the **OK** Button.

Note Up to 50 characters can used for the device name.

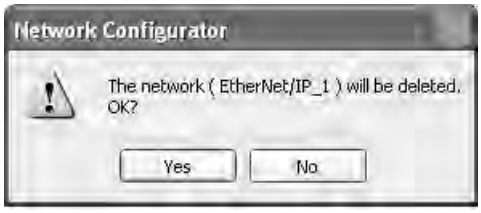
Deleting a Device

It is possible to delete a device from the virtual network.

Procedure

1,2,3...

1. Select the device to delete.
2. Select ***Delete*** from the Edit menu.
   You can also click the Delete Button on the toolbar.
   You can also select the device and click the **Delete** Button on the toolbar.
   Or, right-click the device and select ***Delete***.
   A dialog box will be displayed to confirm the deletion.

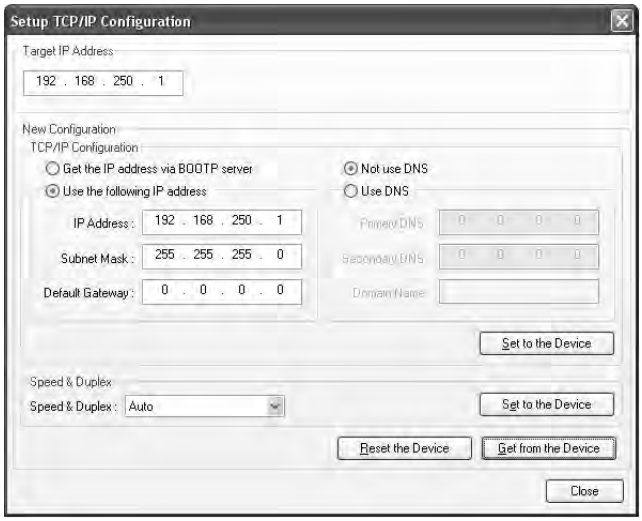


3. Press the **Yes** Button to delete the device.

12-3-3 TCP/IP Settings

Make the TCP/IP settings of the EtherNet/IP Unit, such as the local IP address and subnet mask.

The settings in the Setup TCP/IP Configuration Dialog Box are shown below.



Refer to *5-2-3 EtherNet/IP Communications* EtherNet/IP Communications for information on settings for TCP/IP.

Operation will be performed with the following default values if the NE2A-ENS21 is mounted to the NE2A CPU Unit and the TCP/IP settings have not been made from the Network Configurator.

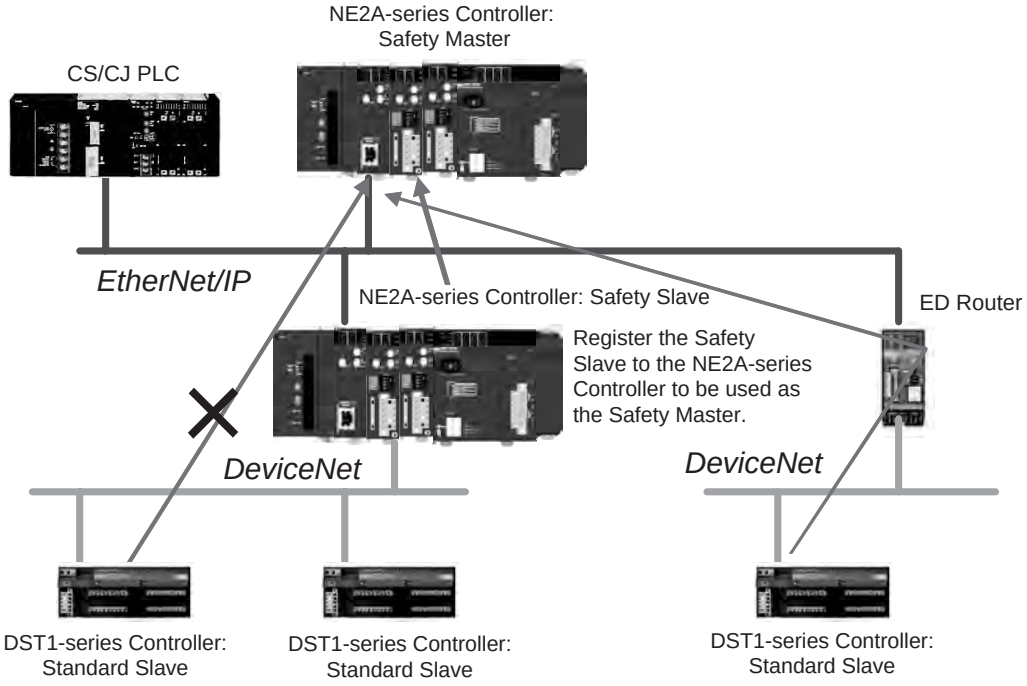
Setting	Operating status
IP address	192.168.250.*node_address*
Subnet mask	255.255.255.0 (IP routing not supported.)
Default gateway	None
Preferred DNS server	None
Alternate DNS server	None
Host name	None
Domain name	None
Speed & Duplex	Automatically detected.

12-4 Communications between an NE2A-series Controller and a Safety Slave

This section described how to make settings to perform communications with a Safety Slave using an NE2A-series Controller as a Safety Master in an EtherNet/IP network.
To operate the NE2A-series Controller as a Safety Master, register the device that is to operate as a Safety Slave and set the connection.

12-4-1 Registering Safety Slaves

Register the Safety Slave to communicate with and set the connection.
This section describes how to set a Safety Connection with a DeviceNet or EtherNet/IP network that has already been built. Refer to *5-4-2 Setting Safety Connections* for information on Safety Connections.

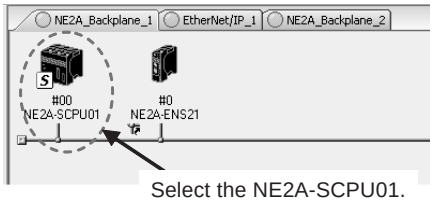


Note (1) With NE2A-series Controllers, routing for DeviceNet networks and EtherNet/IP cannot be performed. An NE1A-EDR01 ED Router is required to route between a DeviceNet network and an EtherNet/IP network.

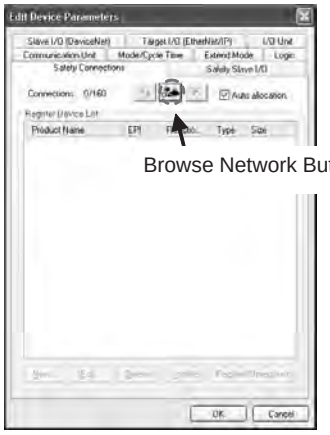
(2) When using the NE2A-series Controller as a Safety Slave, an I/O assembly for a Safety Slave must be registered to set a Safety Connection with the Safety Master. (Refer to *12-5-1 Registering I/O Assemblies for Safety Slaves*.)

Procedure

1,2,3... 1. Select the NE2A-SCPU01 to set in the NE2A Backplane Tab Page of the Network Configuration Pane.



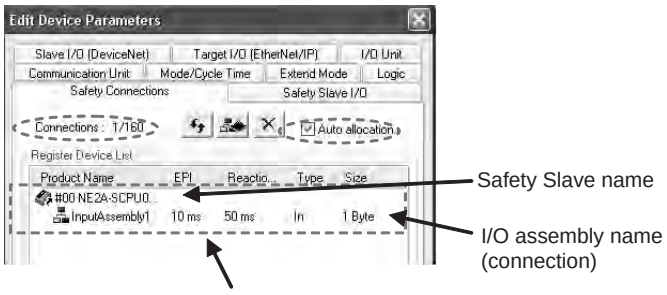
2. Select ***Parameters - Edit*** from the Device Menu.
   You can also right-click the NE2A-SCPU01 device and select ***Parameters - Edit*** from the menu.
   Or, you can double-click the NE2A-SCPU01 device.
   The Edit Device Parameters Dialog Box will be displayed.



3. Click the **Browse Network** Button ( ).
   The Browse Network Dialog Box will be displayed.



4. Select the Safety Slave and click the **OK** Button.
   The Safety Slave will be displayed in the list of registered devices on the Safety Connections Tab Page in the Edit Device Parameter Dialog Box



The following information is displayed in the list of registered devices.

Item	Description
Product Name	The name of the registered Safety Slave (icon) and the name of the I/O assembly used in the set Safety Connection (icon) are displayed.
EPI	The EPI of the Safety Connection is displayed.
Reaction Time	The network response time of the Safety Connection is displayed.
Type	The type of I/O assembly used by the Safety Connection is displayed. In: Input assembly (Slave to Master) Out: Output assembly (Master to Slave)
Size	The size of I/O assembly data used by the Safety Connection is displayed.

- Here the *Auto allocation* Option is selected at the upper-right of the tab page, so the default connection (I/O assembly) of the Safety Slave will be registered when the Safety Slave is registered. (If this option is not selected, the connection will not be registered and the name of the I/O assembly will not be displayed.)
- The number of connections over the number of connections that can be used is displayed in the upper-left part of the tab page.

Note (1) A maximum of 160 connections can be registered. (A maximum of 128 connections can be set for one EtherNet/IP Unit.)

(2) When an NE2A-series Controller is registered as a Safety Slave, the default I/O assembly will not be set.

Adding, Deleting, Editing, and Automatically Registering or Unregistering Connections

The procedures for adding, deleting, editing, and automatically registering or unregistering connections are the same as the procedures for DeviceNet Safety. For details, refer to *11-4-1 Registering Safety Slaves*.

Note The program may be affected if the safety logic connection setting is changed. After making the change, open the Logic Editor and check the program.

12-4-2 Setting Safety Connection Parameters

The procedure for setting Safety Connection parameters is the same as the procedure for setting DeviceNet Safety. For details, refer to *11-4-2 Setting Safety Connection Parameters*.

12-4-3 Convenient Functions for Editing Connections

Editing All Connections

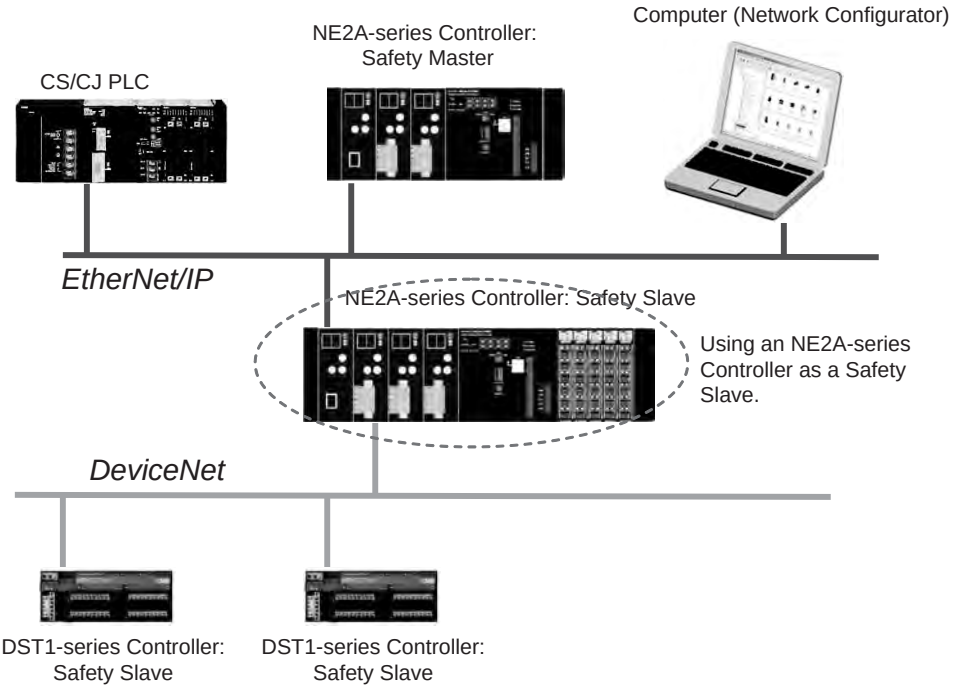
You can display the connection information for all currently set devices in a table and change the parameters. It is not possible to make new connections or to delete existing connections. For details, refer to *11-4-3 Convenient Functions for Editing Connections*.

12-4-4 Stopping or Restarting Communications after an Error

With the NE2A Series, the user can specify whether to stop or continue I/O communications if a connection timeout occurs during Safety I/O Communications with a Safety Slave. If I/O communications are stopped because of a timeout error, the communications can be restarted from the Support Software or the logic program. For details, refer to *11-4-4 Stopping or Restarting Communications after an Error*.

12-5 Using the NE2A-series Controller as a Safety Slave

This section describes how to make settings to use an NE2A-series Controller as a Safety Slave in an EtherNet/IP network.
Set an I/O assembly for a Safety Slave to operate the NE2A-series Controller as a Safety Slave. The I/O assembly can be selected with an NE2A-series Controller as the Safety Master. Variables and I/O tags can be used in the Logic Editor.



Note (1) This setting is not required if the NE2A-series Controller is not used as a Safety Slave.

(2) An NE1A-series Controller cannot be used as a Safety Master for an NE2A-series Controller.

12-5-1 Registering I/O Assemblies for Safety Slaves

Register I/O assemblies for a Safety Slave to enable an NE2A-series Controller to function as a Safety Slave. For details on the procedure, refer to *11-5-1 Registering I/O Assemblies for Safety Slaves*.

12-5-2 Setting Assembly Data

This section describes how to define data for I/O assemblies. For details on the procedure, refer to *11-5-2 Setting Assembly Data*.

12-5-3 Registering I/O Assembles from the Logic Editor

You can register I/O assemblies from the Logic Editor. For details on the procedure, refer to *11-5-3 Registering I/O Assemblies from the Logic Editor*.

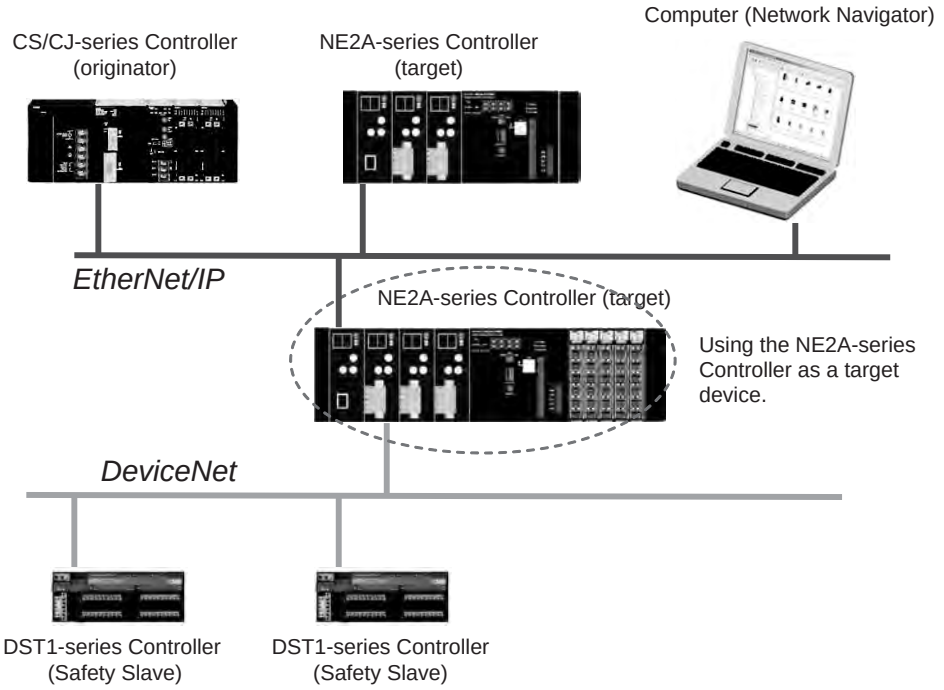
12-6 Communications between the NE2A-series Controller and Standard Slaves

The EtherNet/IP Standard Communications of NE2A-series Controllers support only Target functionality. They do not support Originator functionality. Therefore, setting functionality for Standard Connections is not supported.

For information on setting Standard Connections, refer to the manual for the Communications Unit to be connected for the NE2A-series Controller.

12-7 Using an NE2A-series Controller as a Standard Slave

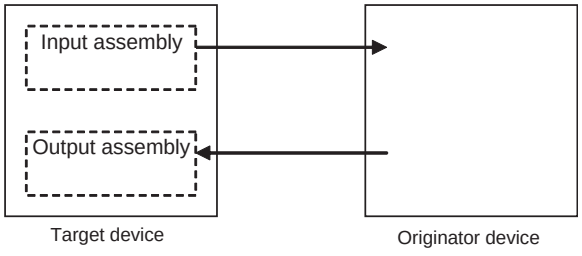
This section describes how to make settings to use the NE2A-series Controller with Target functionality in an EtherNet/IP network.
To operate an NE2A-series Controller with Target functionality, create an I/O assembly as a Target link. The I/O assembly can be selected with a CS/CJ-series Controller that has Originator functionality.



Note This setting is not required if the NE2A-series Controller will not be used as a Target device.

12-7-1 Registering I/O Assemblies for Target Devices

Register I/O assemblies for a Target devices to enable NE2A-series Controllers to function as Target devices. The input assembly is data from the Target device to the Originator device. The output assembly is data from the Originator device to the Target device.



Note Up to 2 input assemblies and 2 output assemblies can be registered for a Target device.

Procedure

1,2,3... 1. Select the NE2A-SCPU01 to be used as the Target device.

2. Select ***Parameter - Edit*** from the Device Menu.
   You can also right-click the NE2A-SCPU01 device to use as the Target device and select ***Parameter - Edit*** from the menu.
   Or, you can double-click the NE2A-SCPU01 device to use as the Target device.
   The Edit Device Parameter Dialog Box will be displayed.
3. Click the **Target I/O (EtherNet/IP)** Tab.
   The Target I/O (EtherNet/IP) Tab Page on the Edit Device Parameters Dialog Box will be displayed.



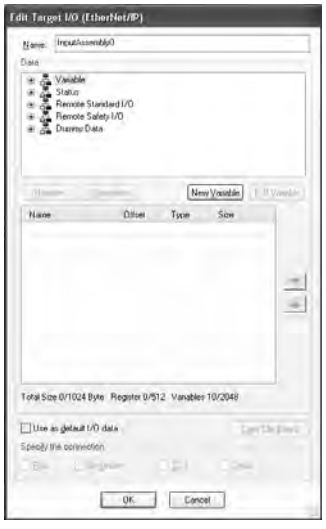
The following information is displayed on the Target I/O (EtherNet/IP) Tab Page.

Item	Information displayed
Name	The name of the registered I/O assembly ( ) and the name of the I/O tag defined in the assembly ( ) are displayed.
Type	The type of I/O assembly (i.e., input or output) and the data type of the I/O tag are displayed.
Size	The size of the I/O assembly and the size of each I/O tag are displayed.

Adding an Input Assembly

Procedure

1,2,3... 1. Click the **New Input** Button on the Target I/O (EtherNet/IP) Tab Page.
The Edit Target I/O (EtherNet/IP) Dialog Box will be displayed.



2. Set the data for the input assembly and click the **OK** Button.
   Refer to *12-7-2 Setting I/O Assemblies* to set the I/O assembly data.

Adding an Output Assembly

Procedure

1,2,3...

1. Click the **New Output** Button on the Target I/O (EtherNet/IP) Tab Page.
   The Target I/O (EtherNet/IP) Dialog Box will be displayed.
   The subsequent steps are the same as those given above in *Adding an Input Assembly*.

Changing I/O Assemblies

Procedure

1,2,3...

1. Select the I/O assembly to be changed.
2. Click the **Edit** Button on the Target I/O (EtherNet/IP) Tab Page.
   The Edit Target I/O (EtherNet/IP) Dialog Box will be displayed.
3. Change the I/O assembly data and click the **OK** Button.
   Refer to *12-7-2 Setting I/O Assemblies* to set the I/O assembly data.

Deleting I/O Assemblies

Procedure

1,2,3...

1. Select the I/O assembly to be deleted.
2. Click the **Delete** Button on the Target I/O (EtherNet/IP) Tab Page.
   A dialog box will be displayed to confirm the deletion.

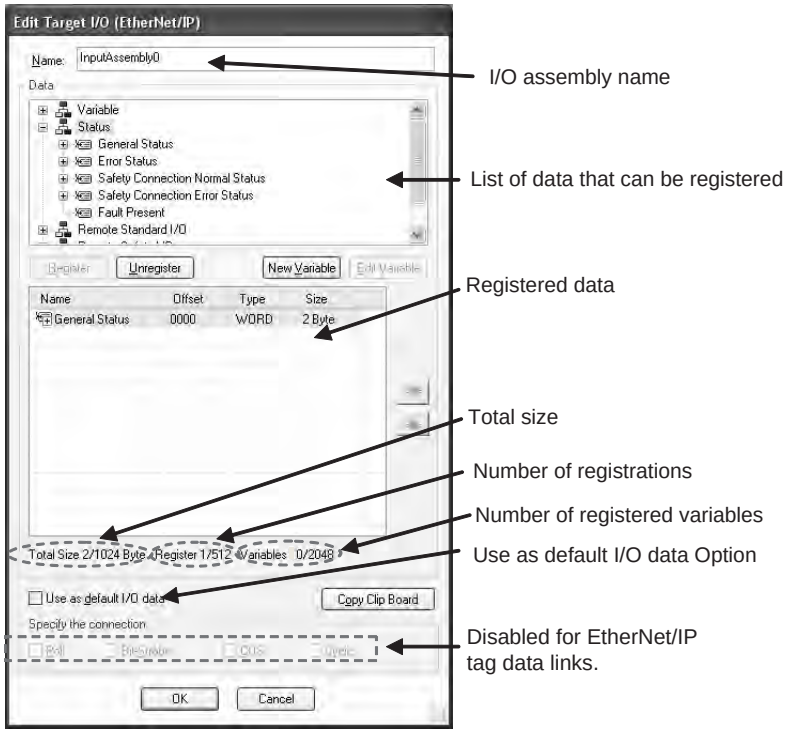


3. Click the **OK** Button.
   The I/O assembly will be deleted.

12-7-2 Setting I/O Assemblies

This section describes how to define data for I/O assemblies.

Edit Target I/O (EtherNet/IP) Dialog Box



I/O Assembly Name

The I/O assembly name can be edited.

Note An I/O assembly name can contain up to if 48 characters.
The characters that can be input are the same as those that can be input for variables. Refer to *Variable Specifications* on page 80.

List of Data That Can Be Registered

This list displays the data that can be registered to I/O assemblies.
For details, refer to *5-8-2 Configuring Assemblies*.

Note Dummy data is used if the Master can transfer only an even number of bytes.

Registered Data List

This list displays data that was registered from the list of data that can be registered.
The following information is displayed in the Registered data List.

Item	Information displayed
Name	The name of the registered data is displayed.
Offset	The position in I/O assembly data of allocated data is displayed
Type	The type of the registered data is displayed.
Size	The size of the registered data is displayed.

Total Size

This area displays the total size of the I/O assembly. A maximum of 1,024 bytes can be registered for one input assembly and 1,024 bytes for one output assembly.

Note The data size will be set as one byte if the data size is less than one byte, e.g., for BOOL variables and local I/O input data.

Number of Registrations

The number of data items registered to the I/O assembly is displayed here. A maximum of 64 status information items can be registered for one input assembly and 64 for one output assembly.

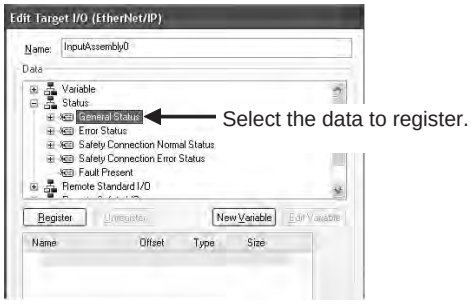
Use as Default I/O Data Option

Use this option to specify the default connection. Connections of I/O assemblies for which this option is selected will be automatically registered when automatic allocation is used and registration is performed with the Originator.
If this option is selected for an I/O assembly, the selection will be cleared for the I/O assembly for which it was previously selected.

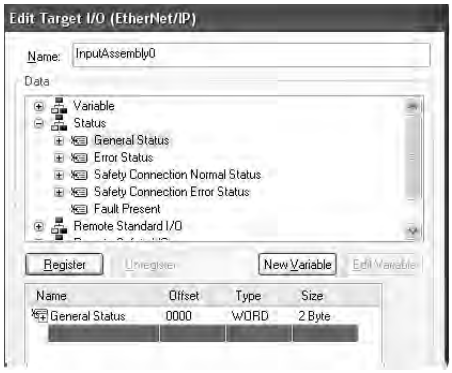
Registering Data

Procedure

1,2,3... 1. Select the data to register from the list of data that can be registered.



2. Click the **Register** Button. The data will be displayed in the list of registered data.

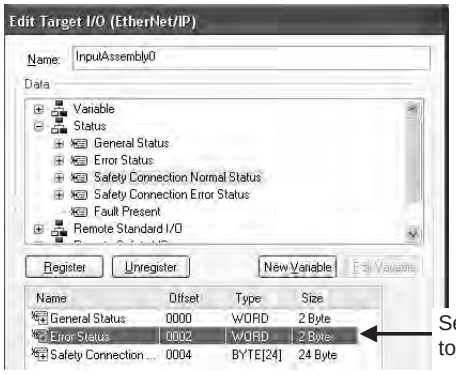


The total size and the number of registrations will be updated.

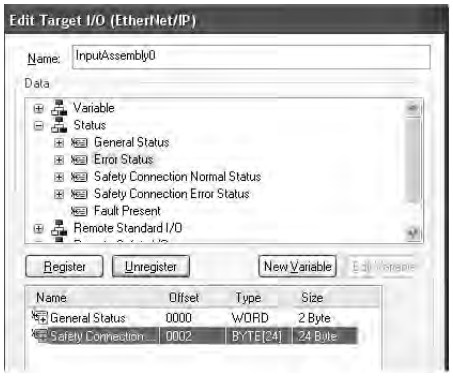
Unregistering Data

Procedure

1,2,3... 1. Select the data to unregister from the list of registered data.



2. Click the **Unregister** Button. The data will be unregistered and deleted from the list of registered data.



The total size and number of registrations will be updated.

Creating New Variables

I/O assembles can be created in the Target I/O (EtherNet/IP) Dialog Box. It is also possible to create variables to register to I/O assembles with the Logic Editor. Refer to *15-5 Creating Variables* for information on creating variables with the Logic Editor.

Procedure

1,2,3... 1. Click the **New Variable** Button in the Target I/O (EtherNet/IP) Dialog Box. The New Variable Dialog Box will be displayed.

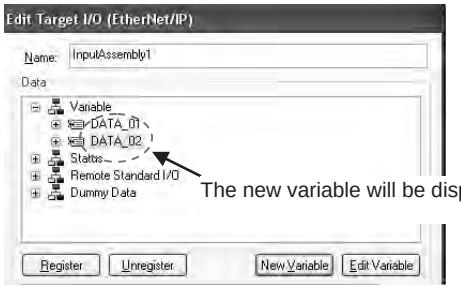


2. Set the variable data and click the **OK** Button. The following table describes the settings in the New Variable Dialog Box.

Settings	Description
Name	Specifies the variable name. Up to 48 characters (48 bytes max.) can be used. Names are not case sensitive if ASCII alphanumeric characters are used. The following characters cannot be used: : ! # $ % & ' " ( ) = ~ ^ \ | ` @ { + ; * : } < , > ? / . [ ] Also the following cannot be used: • The first character cannot be a number. • Reserved characters cannot be used.
Data type	Select from BOOL, BYTE, WORD, or DWORD.

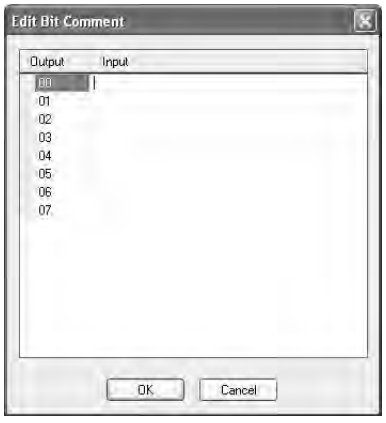
The Edit Bit Comment button will be enabled if BOOL is not selected for the data type. (For details, refer to *Editing Bit Comments* on page 304 in the following section.)

A new variable will be added to the list of data that can be registered in the Target I/O (EtherNet/IP) Dialog Box.



Editing Bit Comments

1,2,3... 1. Click the **Edit Bit Comment** Button.
The Edit Bit Comment Dialog Box will be displayed.



2. Enter a comment for each bit and press the **Enter** Key.
3. Click the **OK** Button. The bit comments will be set.

Note Up to 48 characters (48 bytes) can used for the bit comment.
The characters that can be input are the same as those that can be input for variables. Refer to *Variable Specifications* on page 80.

Editing

You can edit registered variables. For information on the procedure, refer to *Creating New Variables* on page 303 above.

Changing the Order of Registered Data

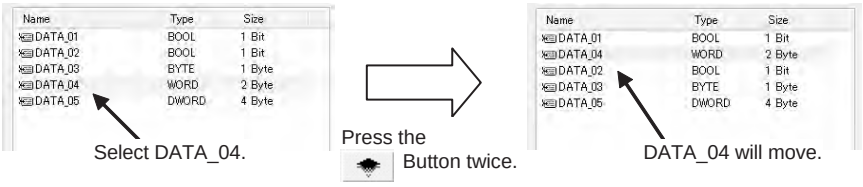
You can change the order of registered data.

Procedure

1,2,3... 1. Select the registered data that you will change the order of.

2. Click the Button (move up) or Button (move down). The registered data that is selected will move.

Example:



Note BOOL data can be arranged in BYTE, WORD, or DWORD data. If longer variables, such as BYTE variables, are placed between continuous BOOL variables, the total data size will change.

12-7-3 Registering I/O Assemblies from the Logic Editor

You can register I/O assemblies from the Logic Editor.

Procedure

1,2,3... 1. Select ***Setting - Target I/O*** from the Device Menu of the Logic Editor. The Target/Slave I/O Settings Dialog Box will be displayed.

2. Click the **Target I/O (EtherNet/IP)** Tab. The Target I/O (EtherNet/IP) Tab Page will be displayed in the Target/Slave Settings Dialog Box.



3. Click the **New Input** Button or **New Output** Button. The Edit Target I/O (EtherNet/IP) Dialog Box will be displayed.

The procedures for adding, changing, and deleting I/O assemblies are the same as the procedures for Target devices. For details, refer to *12-7-1 Registering I/O Assemblies for Target Devices*.

12-7-4 Setting Slave Input Data in IDLE Mode

You can set to hold or clear the previous data in any of the following cases for input assembles transferred from an NE2A-series Standard Slave to a Standard Master.

- The NE2A-series Controller is changed from RUN Mode to IDLE Mode.
- A communications error or other error is detected in a safety chain that sets data to I/O tags of input assemblies.

SECTION 13
Verifying System Performance

This section describes how to verify the performance of a NE2A-series Safety Network Controller system.

13-1 System Performance Verification 308
13-1-1 DeviceNet Performance Verification 309
13-1-2 EtherNet/IP Performance Verification Procedure 310
13-2 Checking the NE2A-series Controller Cycle Time 311
13-2-1 Checking the Instruction Execution Cycle Time and Peripheral Servicing Cycle Time 311
13-3 Checking the Communications Response Performance 313
13-3-1 Checking the Communications Response Performance in a DeviceNet 313
13-3-2 Checking the Communications Response Performance in an EtherNet/IP 320
13-4 Verifying the Safety Response Performance (Reaction Time) 327
13-5 Standard I/O Communications Network Response Performance 329

13-1 System Performance Verification

The user must check that the safety response performance (reaction time) in all the safety chains and the Standard I/O Communications response performance meet the required specifications.

To verify the reaction time in the safety chains and the Standard I/O Communications response performance, check the following NE2A-series Controller parameters.

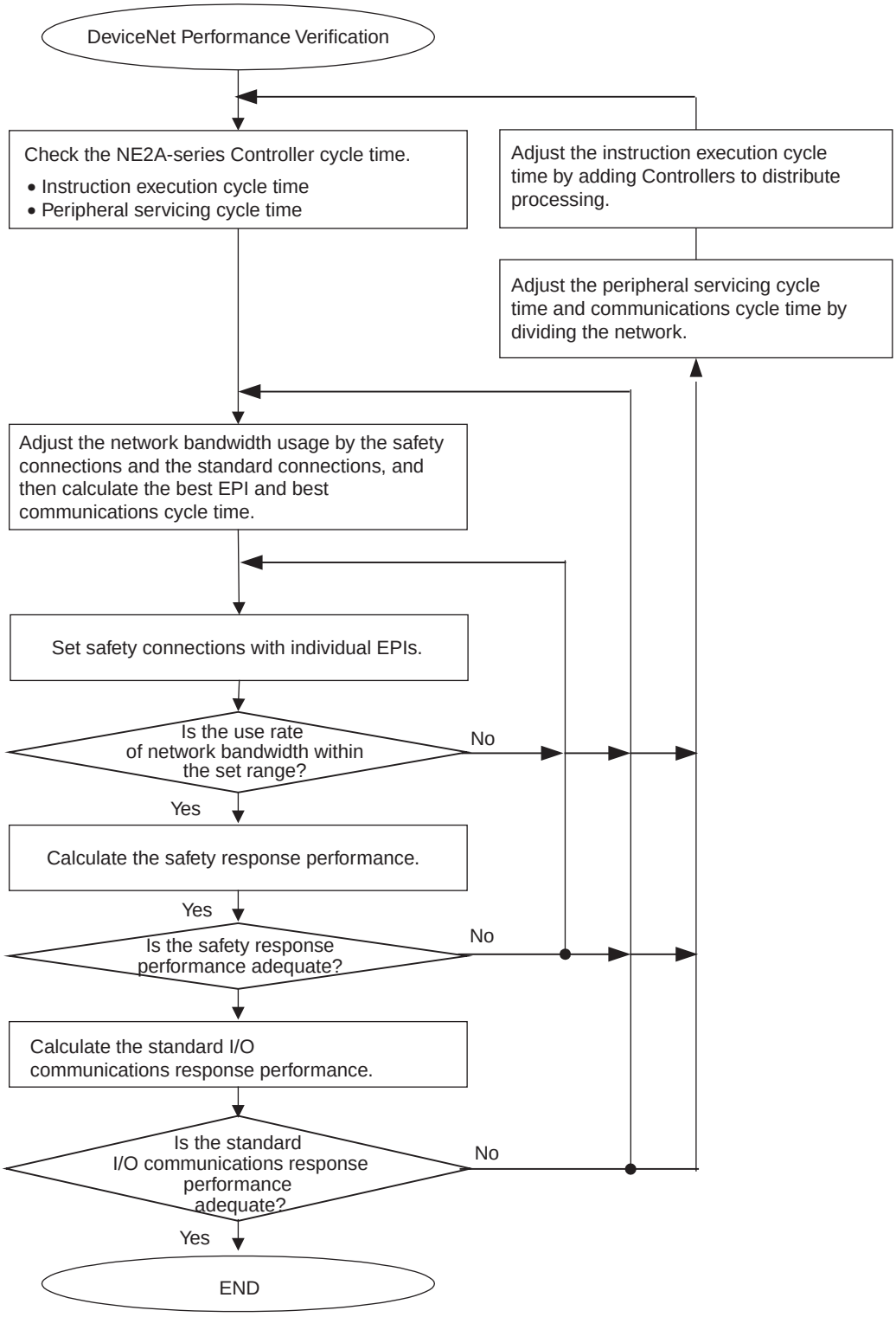
- NE2A-series Controller Instruction Execution Cycle Time
- NE2A-series Controller Peripheral Servicing Cycle Time

For the response performance between communication nodes, also check the following values.

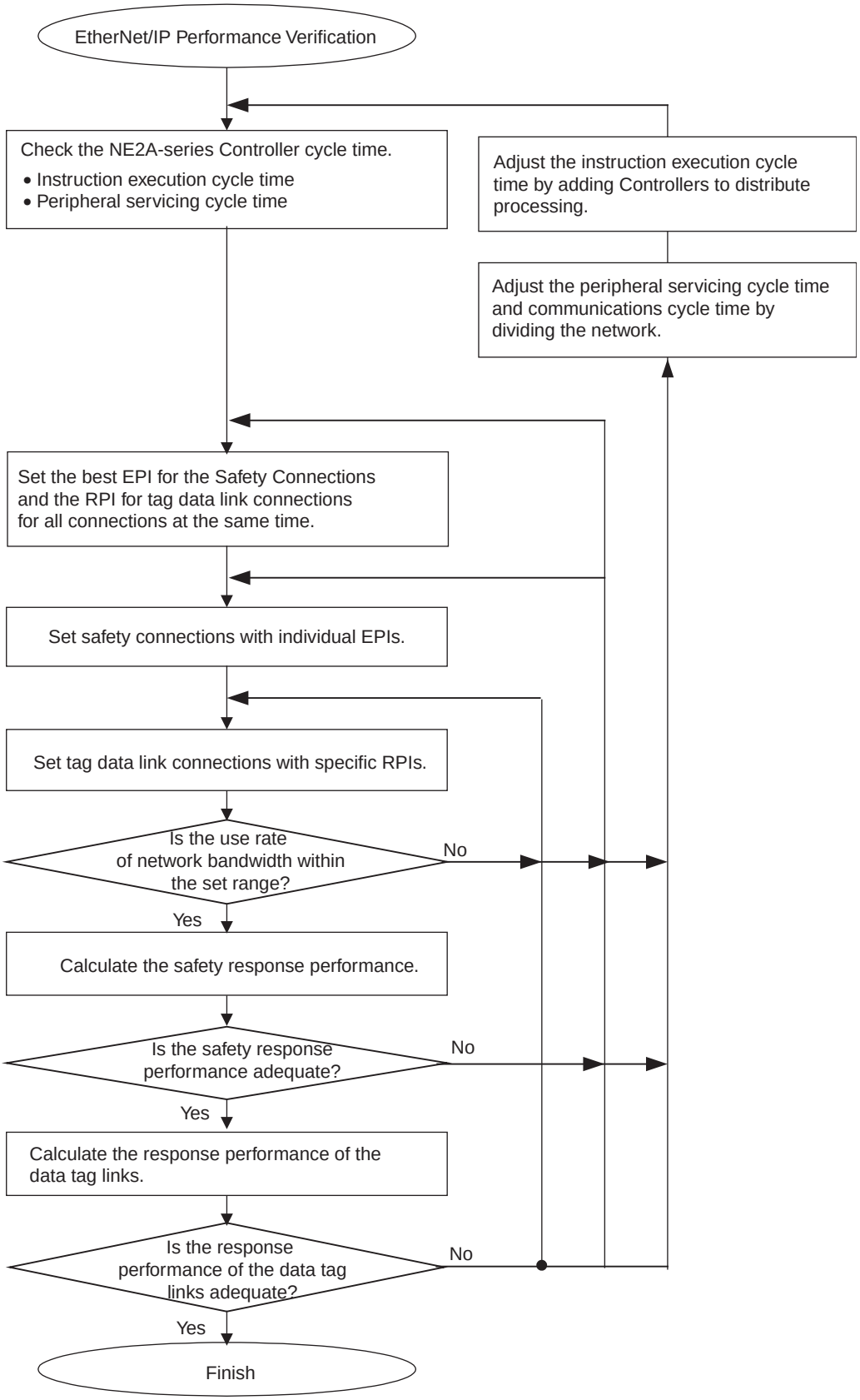
- The network reaction time of Safety I/O Communications in each network.
- The Standard I/O Communications cycle time in each network.

The following diagrams show the steps for verifying the performance of DeviceNet and EtherNet/IP systems.

13-1-1 DeviceNet Performance Verification



13-1-2 EtherNet/IP Performance Verification Procedure



13-2 Checking the NE2A-series Controller Cycle Time

The user must check the following three cycle times of the NE2A-series Controller. They are required for the trial calculation of the safety response performance (reaction time) and Standard Communications response performance.

- Instruction Execution Cycle Time
- Peripheral Servicing Cycle Time

Refer to *SECTION 8 Calculating System Performance* for details of each cycle time.

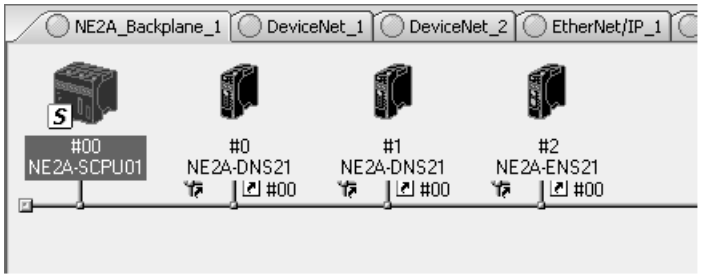
13-2-1 Checking the Instruction Execution Cycle Time and Peripheral Servicing Cycle Time

The instruction execution cycle time and peripheral servicing cycle time are automatically calculated by the Network Configurator. The NE2A-series System program must be created to calculate the instruction execution cycle time. The Communications Unit's configuration and connections must be set to calculate the peripheral servicing cycle time.

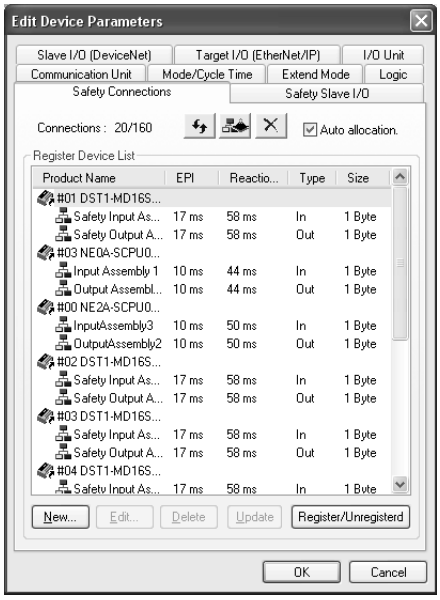
Use the following procedure to check the instruction execution cycle time and the peripheral servicing cycle time.

Procedure

1,2,3... 1. Select the Target NE2A-series CPU Unit.



2. Select ***Device - Parameter - Edit***. The Edit Device Parameters Dialog Box will be displayed.



3. Click the **Mode/Cycle Time** Tab and check the Instruction Execution Cycle Time and Peripheral Servicing Cycle Time.



The instruction execution cycle time and peripheral servicing cycle time can be set within the ranges indicated below as long as they are above the values calculated by the Network Configurator.

- Instruction Execution Cycle Time
  From the value calculated by the Network Configurator to 50 ms (0.1-ms increments)
- Peripheral Servicing Cycle Time
  From the value calculated by the Network Configurator to 100 ms (0.1-ms increments)

13-3 Checking the Communications Response Performance

The user must check the following performance items to verify the safety response performance (reaction time) and Standard I/O Communications response performance.

- The network reaction time and Standard I/O Communications cycle time in a DeviceNet network
- The network reaction time and RPI (requested packet interval) in an EtherNet/IP network

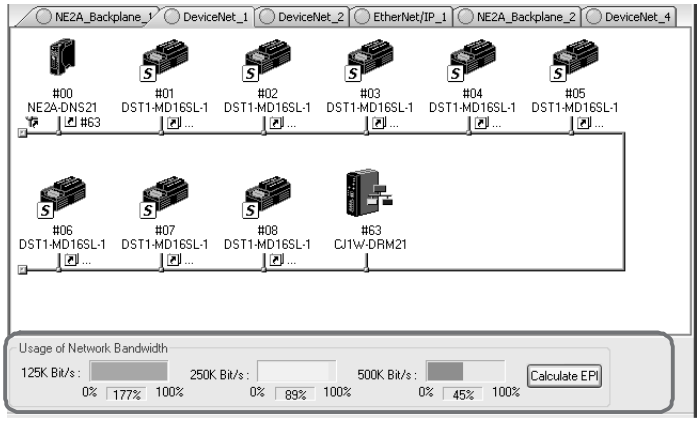
13-3-1 Checking the Communications Response Performance in a DeviceNet

When the network bandwidth used by Safety I/O Communications and Standard I/O Communications in a DeviceNet are set by the Network Configurator, the best average EPI (expected packet interval) and best Standard I/O Communications cycle time are calculated. In turn, when the EPI is set, the network reaction time for Safety Connections is automatically calculated by the Network Configurator.

The network reaction time and the best Standard I/O Communications cycle time will be calculated for each DeviceNet network. In this example it is assumed that all registered Slaves and connections in the Target DeviceNet network have already been set.

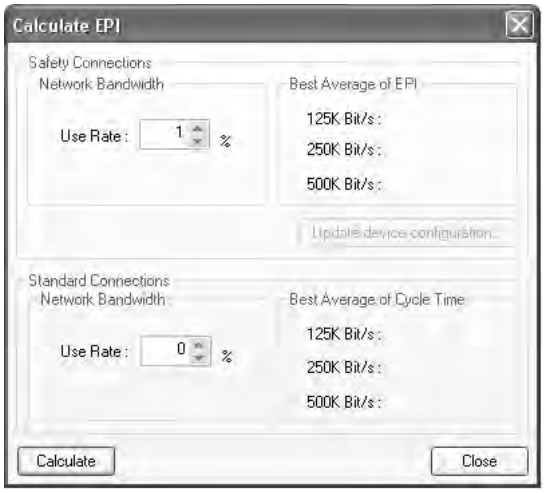
Procedure

1,2,3... 1. Click the Target **DeviceNet** Tab in the Network Configuration Pane.
The following dialog box will be displayed.



The Network Configurator displays the actual network bandwidth usage rate for Safety I/O Communications and Standard I/O Communications at the bottom of the Network Configuration Pane under *Usage of Network Bandwidth for Safety Connections*. The higher the baud rate, the less bandwidth is used.

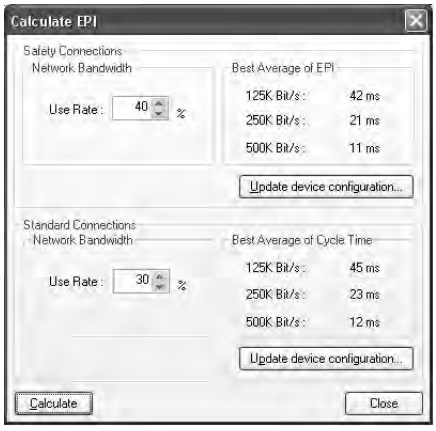
2. Click the **Calculate EPI** Button at the bottom of the Network Configuration Pane.
The Calculate EPI Dialog Box will be displayed.



3. Set the Network Bandwidth Use Rate for Safety Connections and Standard Connections.
   - Using Only Safety I/O Communications:
     Input the network bandwidth used by the Safety Connections as 90% or less and input 0% for the network bandwidth used by Standard Connections.
   - Using Both Safety and Standard I/O Communications:
     Input the total network bandwidth used for Safety Connections and Standard Connections as 90% or less, e.g., 40% for Safety Connections and 30% for Standard Connections. Safety and Standard I/O Communications will use the bandwidth based on the rates specified here.

Note Keep 10% or more of the network bandwidth available for establishing connections and for explicit message communications with the Network Configurator, whether using only Safety I/O Communications or using both Safety I/O and Standard I/O Communications. Even if 10% or more is available, however, safety or Standard Communications might time out due to the Network Configurator operation (e.g., monitoring or other operations that create a load on the network) or if the user application uses explicit message communications. If timeouts occur, reduce the network bandwidth usage rate (i.e., increase the unused bandwidth).

4. Click the **Calculate** Button.
   The best average of EPI of all the connections in the Safety I/O Communications and the optimum Master cycle time in the Standard I/O Communications will be calculated and displayed for each baud rate.



Change the EPI settings for each Safety Connection and the Standard I/O Communications cycle time for the Standard Master.

Changing the EPI for Each Safety Connection

The Best Average EPI is the average value of all the Safety Connections in the target DeviceNet network.

First, check whether the EPI corresponding to the baud rate that is being used is longer than following times.

1. The peripheral servicing cycle time of the NE2A-series CPU Unit
2. The EPI for which operation is possible for Safety I/O Communications for the NE2A-series DeviceNet Unit
3. The cycle time of the Safety Slave (DST1 Slave: 6 ms, NE0A Slave: 7 ms min.)

The maximum value of the above times is the minimum value that can be set for the EPI.

You can check the NE2A-series CPU Unit's peripheral servicing cycle time by following the procedure outlined in *13-2-1 Checking the Instruction Execution Cycle Time and Peripheral Servicing Cycle Time*.

The calculated result will be set as the EPI for all Safety Connection parameters in the DeviceNet. The values can be changed later as required for individual connections.

Procedure

1,2,3... 1. Click the **Update Device Configuration** Button.
The Update Device Configuration Dialog Box will be displayed.



2. Select the Baud Rate to use and click the **OK** Button.

With this procedure it is possible to set the EPI for all Safety Connections on the target DeviceNet network.

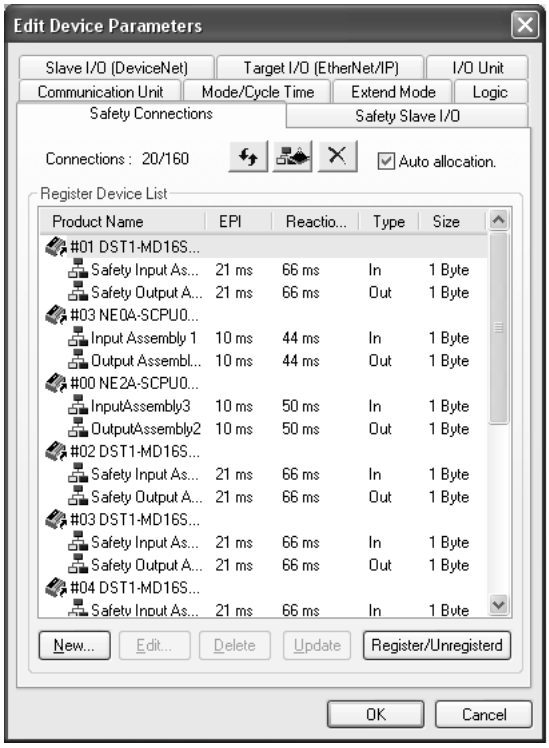
Note Select the *Custom EPI* Option in the User setup Area when setting an EPI value that is not automatically calculated.

Next, adjust the EPI for each Safety Connection.

3. Click the **Close** Button in the Calculate EPI Dialog Box.
4. Select the target NE2A DeviceNet Unit in the Network Configuration Pane, and then select ***Device - Display Routing Network***.

   The NE2A_Backplane for the NE2A CPU Unit with a mounted DeviceNet Unit will be displayed.
5. Select the NE2A-series CPU Unit and select ***Device - Parameters- Edit***.

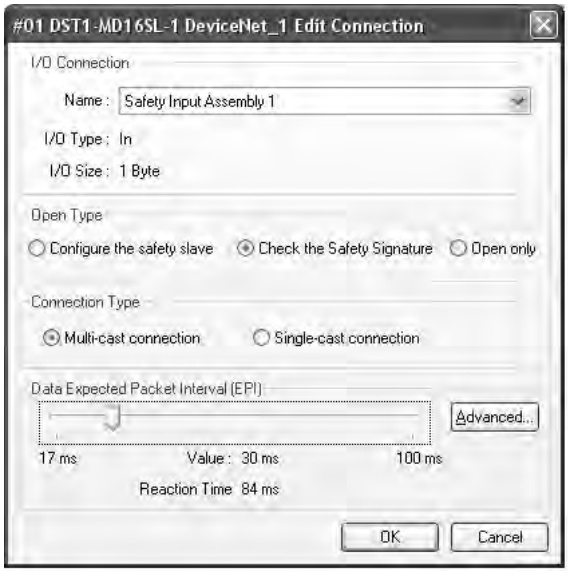
   The following Edit Device Parameters Dialog Box will be displayed.



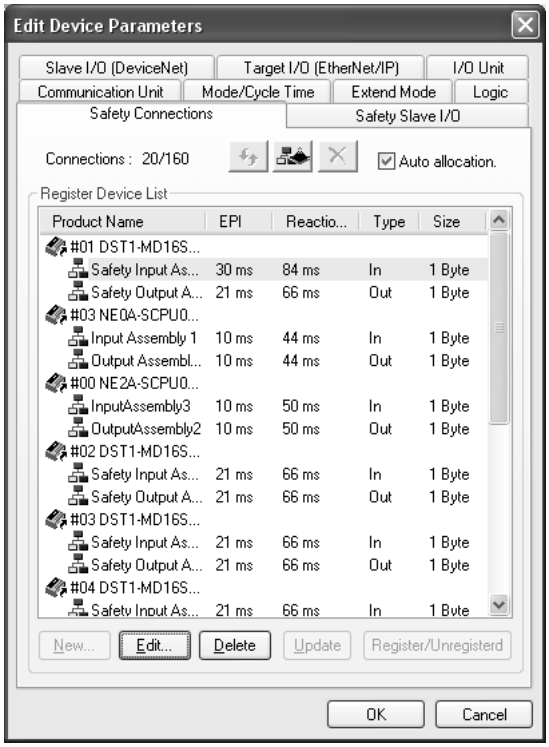
The calculated Best Average EPI value will be set as the EPI in all Safety Connection parameters in the Target DeviceNet.

If required, adjust the EPI setting for the whole network, making the EPI smaller for those connections that need a faster reaction time (e.g., Safety Curtain connections) and making the EPI larger for those connections that do not need a fast reaction time (e.g., for door switches not used in hazardous areas).

6. Select a connection to adjust and click the **Edit** Button.
   The following Edit Connection Dialog Box will be displayed for the selected connection.



7. Set the EPI using the slider in the Data Expected Packet Interval.
   The network reaction time can be checked under Reaction Time in the Data Expected Packet Interval field.
8. Click the **OK** Button.
   The EPI of the selected connection will be changed.



Note

- Set the EPI for each Safety Connection to a value that is larger the maximum value of the following times.

1. The peripheral servicing cycle time of the NE2A-series CPU Unit
2. The EPI for which operation is possible for Safety I/O Communications for the NE2A-series DeviceNet Unit

3. The cycle time of the Safety Slave (DST1 Slave: 6 ms, NE0A Slave: 7 m min.)
   - When using Slave operation to communicate with a NE2A/NE1A/NE0A-series Controller, the cycle time of the Controller will not be checked. Use the Network Configurator to check that the EPI value is longer than the NE2A/NE1A/NE0A-series Controller cycle time.

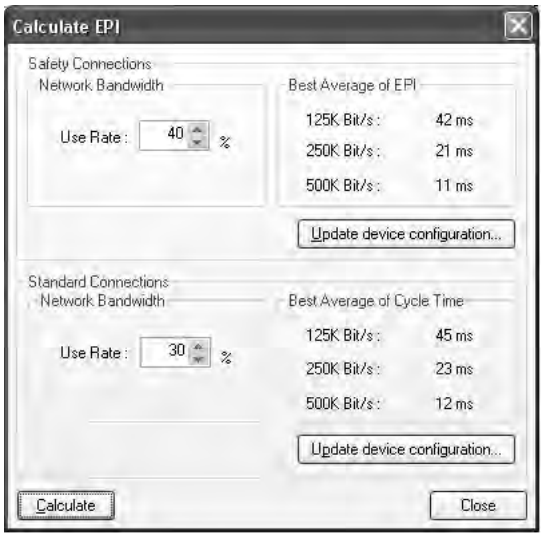
Changing the Communications Cycle Time for Standard I/O Communications

The resulting calculated best average cycle time for standard connections is the best Standard I/O Communications cycle time.

Set the result of calculation as the Standard I/O Communications cycle time for the Standard Master.

Procedure

1,2,3... 1. Click the **Update device configuration** Button in the *Standard Connection* Field in the Calculate EPI Dialog Box.



The Change Device Settings Dialog Box will be displayed.

2. Select the baud rate to use, and then click the **OK** Button.

   With this procedure is possible to set the Standard I/O Communications cycle time for the Standard Master on the target DeviceNet network.

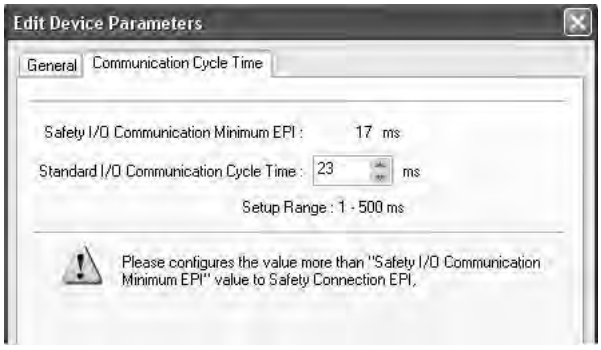
Note Select *Custom EPI* Option in the User setup Area and set the Standard I/O Communications cycle time to set a Standard I/O Communications cycle time that is not automatically calculated.

If an NE2A DeviceNet Unit is used as the Standard Communications Master, the Standard I/O Communications cycle time of the NE2A DeviceNet Unit Standard Communications Master cannot be set to a value lower than the value automatically calculated by the NE2A DeviceNet Unit.

The Standard I/O Communications cycle time for NE2A DeviceNet Units can be checked in the Edit Device Parameters Dialog Box of the NE2A DeviceNet Unit.



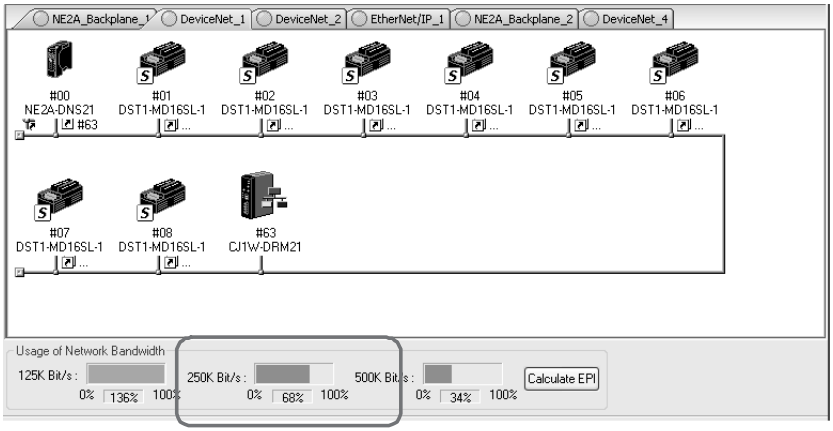
The following message will be displayed in the Message Reporter Pane.



Reconfirming the Bandwidth Use Rate

If the EPI settings in the Safety Connection parameters or the Standard I/O Communications cycle time setting of the Standard Master has been changed based on the calculation results, check that the network bandwidth usage when Safety Connections are used, displayed at the bottom of the Network Configuration Pane, is less than the value input in the Calculated EPI Dialog Box.

It is particularly important to check the bandwidth usage rate if the best average EPI has been adjusted for each connection rather than applied as a batch setting.



Note The EPI is set in 1-ms units, so the network bandwidth usage rate may be smaller than the input value if the calculation result is input directly.

13-3-2 Checking the Communications Response Performance in an EtherNet/IP

The EPIs of the Safety Connections and the RPIs of the Tag Data Links can all be set from the Network Configurator using the Set Packet Interval (RPI) Button. The EPIs of the Safety Connections can also be set individually.

The network reaction times for Safety Connections are automatically calculated by the Network Configurator.

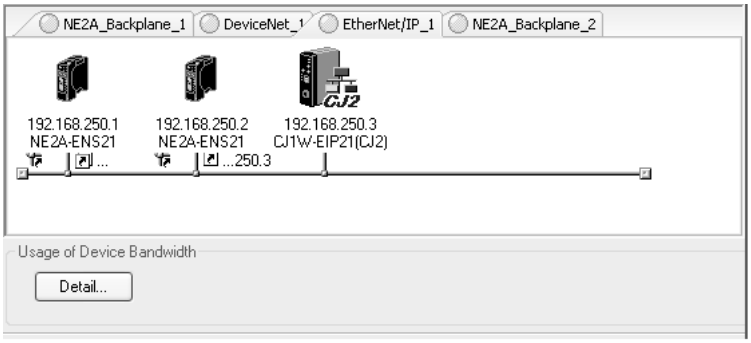
There are two methods that can be used to set the RPIs for Tag Data Links.

- Method 1: The RPIs of all Tag Data Link Connections for a specific device can be set to the same value.
- Method 2: The RPIs for specific Tag Data Link Connections can be set.

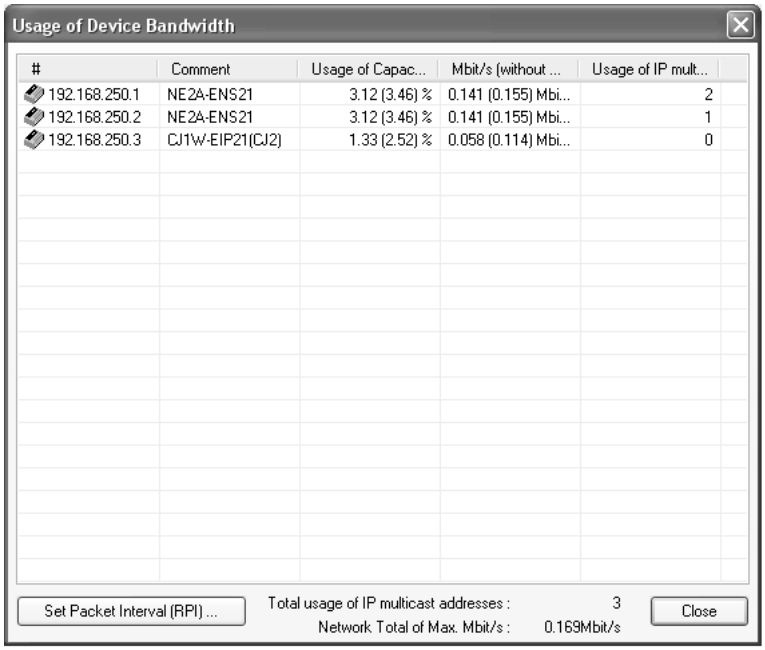
The network reaction times and RPIs are calculated for each EtherNet/IP network. To calculate them, all devices must be registered and all connections must be set in the target EtherNet/IP network.

Procedure

1,2,3... 1. Click the target **EtherNet/IP** Tab in the Network Configuration Pane. The following dialog box will be displayed.



2. Click the **Detail** Button under the Usage of Device Bandwidth. The Usage of Device Bandwidth Dialog Box will be displayed.



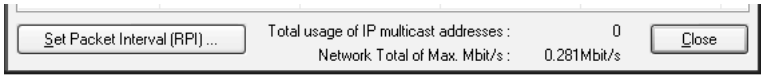
The network bandwidth actually used by the Safety I/O Communications and Tag Data Link will be displayed for each device according to the connections set by the Network Configurator.

- The displayed content is described in the following table.

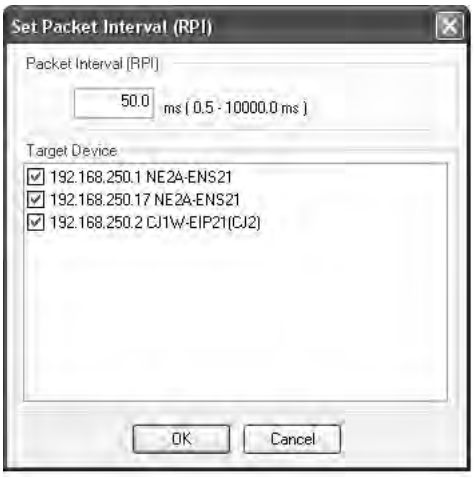
Item	Displayed content or operation
#	IP address
Comment	Device name
Usage of Capacity	Displays the proportion of transferred packets supported by the allowed communications bandwidth of the device. Value outside parenthesis: Proportion of transferred packets when a multicast filter is used. Value inside parenthesis: Proportion of transferred packets when a multicast filter is not used.
Mbits/s	Number of bits processed in 1 second by the device's Ethernet port. Value outside parenthesis: Number of processed bits when a Multicast filter is used. Value inside parenthesis: Number of processed bits when a Multicast filter is not used.
Usage of IP multi-cast address	Number of times the device's multicast address is used.
Total usage of IP multicast addresses	Number of times the whole network's multicast address is used.
Network Total of Max. Mbit/s	The maximum number of bits processed in 1 second by the Ethernet port in the network.
Set Packet Interval (RPI) Button	Sets all of the Safety Connection EPIs and all of the Tag Data Link Connection RPIs.
Close Button	Closes the dialog box.

Note Performing message communications or other network operations from the Network Configurator (such as monitoring or other operations that place a load on the network) or from the user application when the Tag Data Link bandwidth usage of capacity is between 80% and 100% can create an excessive load on the network and result in timeouts. If timeouts occur, increase the EPI and RPI settings or reduce the usage of capacity.

3. Click the **Set Packet Interval (RPI)** Button in the Usage of Device Bandwidth Dialog Box .



The Set Packet Interval (RPI) Dialog Box will be displayed.



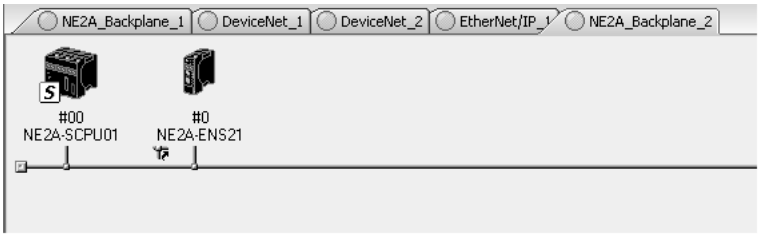
4. Input the packet interval and click the **OK** Button.
   - The EPIs for all Safety Connections in the specified EtherNet/IP networks will be set.
   - The RPIs for all Tag Data Link Connections in the specified EtherNet/IP networks will be set.

Changing the EPI for Each Safety Connection

The EPI can be set for each EtherNet/IP Safety Connection.

Procedure

1,2,3... 1. Select the NE2A-series CPU Unit that has the EtherNet/IP connection to be changed.



2. Select ***Device - Parameter - Edit***.
   The following Edit Device Parameters Dialog Box will be displayed.



Check the EPI values for Safety Connections in the Target EtherNet/IP.

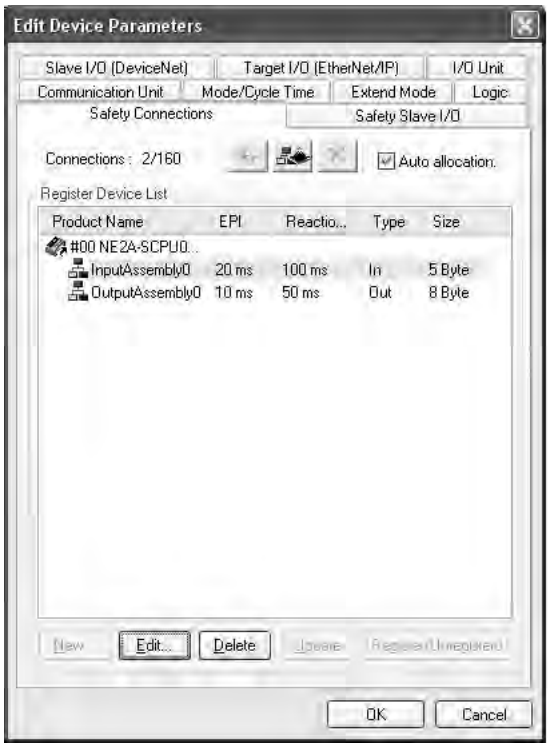
The EPI values will be those set in *12-4-1 Registering Safety Slaves*.

If required, adjust the EPI settings for the whole network, making the EPI smaller for those connections that need a faster reaction time and making it larger for those connections that do not need a fast reaction time.

3. Select the Target EtherNet/IP Safety Connection and click the **Edit** Button.
4. Set the EPI using the slider in the Data Expected Packet Interval.
   The network reaction time can be checked under Reaction Time in the Data Expected Packet Interval field.



5. Click the **OK** Button.
   The EPI of the selected connection will be changed.



6. Set the EPI for all Safety Connections that need to be changed by repeating step 4.

Note

- Set the EPI for each Safety Connection to a value that is higher than the following times.
  a. The peripheral servicing cycle time of the NE2A-series CPU Unit
  b. The cycle time of the Safety Slave
- If the communications partner is an NE2A-series Slave, the cycle time of the communications partner will not be checked. Use the Network Configurator to check that the EPI is longer than the peripheral servicing cycle time of the NE2A -series CPU Unit.

Changing the RPIs of Tag Data Link Connections

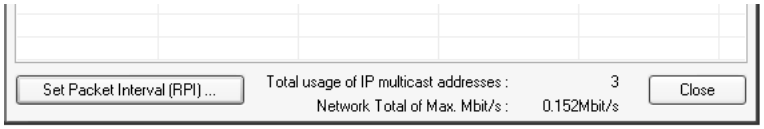
Method 1: Changing a Particular Device's RPI Setting

The Usage of Capacity of the allowed communications bandwidth can be adjusted for a particular device by changing the packet intervals (RPI) for all of the device's Tag Data Link connections together. In this case, the Usage of Capacity will also change for the devices that are the Target devices of the connection which was adjusted.

Procedure

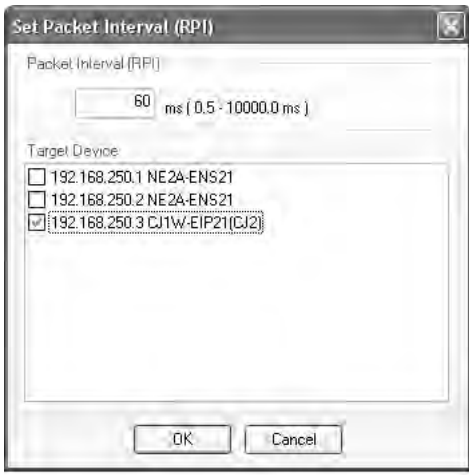
1,2,3...

1. Click the **Set Packet Interval (RPI)** Button in the Usage of Device Bandwidth Dialog Box.



The Set Packet Interval (RPI) Dialog Box will be displayed.

2. In the *Target Device* Area, deselect the Target devices that are not being adjusted by removing the check marks.



3. Input a new Packet Interval (RPI) value, and click the **OK** Button.

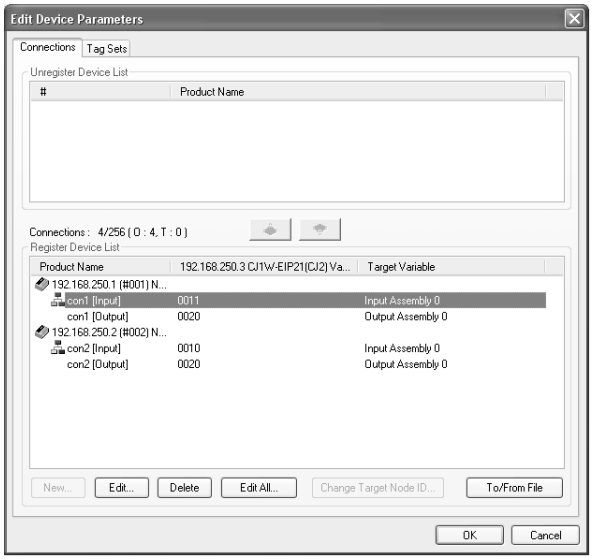
Method 2: Changing a Particular Connection's RPI Setting

The Usage of Capacity of the allowed communications bandwidth can be adjusted by individually changing the packet intervals (RPI) setting for a particular connection. In this case, the Usage of Capacity will also change for the device that is the Target device of the connection which was adjusted.

Procedure

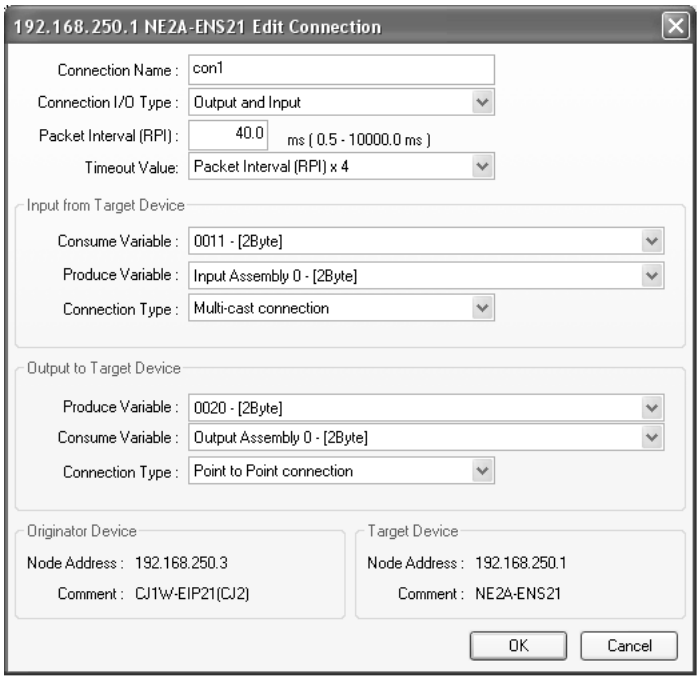
1,2,3...

1. Click the **Close** Button in the Usage of Device Bandwidth Dialog Box to close the dialog box.
2. Select the device that is set as the Originator of the desired connection, and select ***Device - Parameter - Edit***.
   The Edit Device Parameter Dialog Box will be displayed.



3. In the Register Device List, select the connection for which you want to change the packet interval (RPI), and click the **Edit** Button.

   The device's Edit Connections Dialog Box will be displayed.

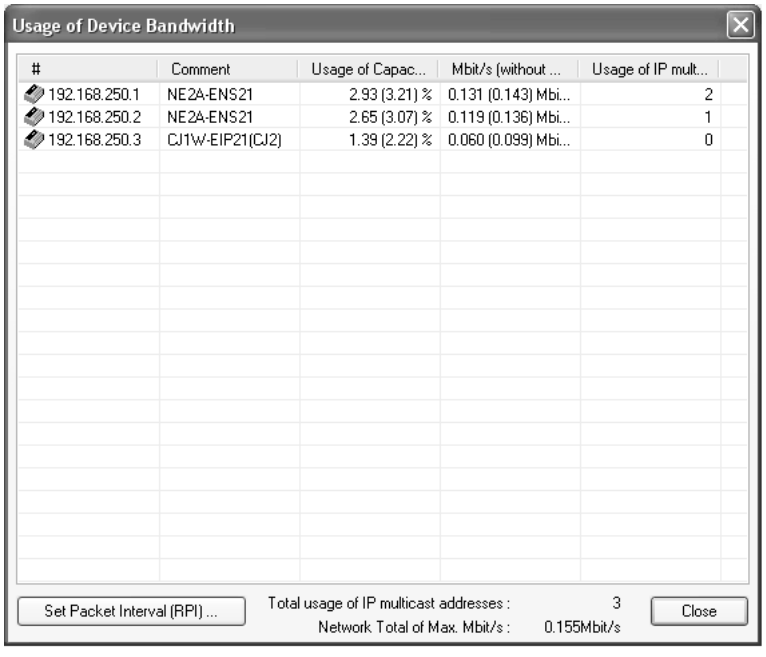


4. Input a new packet interval (RPI) value, and click the **OK** Button.

Reconfirming the Bandwidth Use Rate

If the connection settings have been changed, click the **Detail** Button in the Usage of Device Bandwidth Area at the bottom of the Network Configuration Pane. Verify that the allowed communications bandwidth used (Usage of Capacity) is less than 100% and that the Mbit/s value is less than the baud rate of the Ethernet.

It is particularly important to check the Usage of Capacity when an individual connection's packet interval (RPI) setting was changed rather than all set at the same time.



13-4 Verifying the Safety Response Performance (Reaction Time)

The Network Configurator checks the following values and calculates the safety response performance (reaction time).

- NE2A-series Controller Instruction Execution Cycle Time
- NE2A-series Controller Peripheral Servicing Cycle Time
- Network Reaction Time

Check the safety response performance of each safety chain based on the formulas and calculation examples in *8-2-2 Calculating the Reaction Time*.

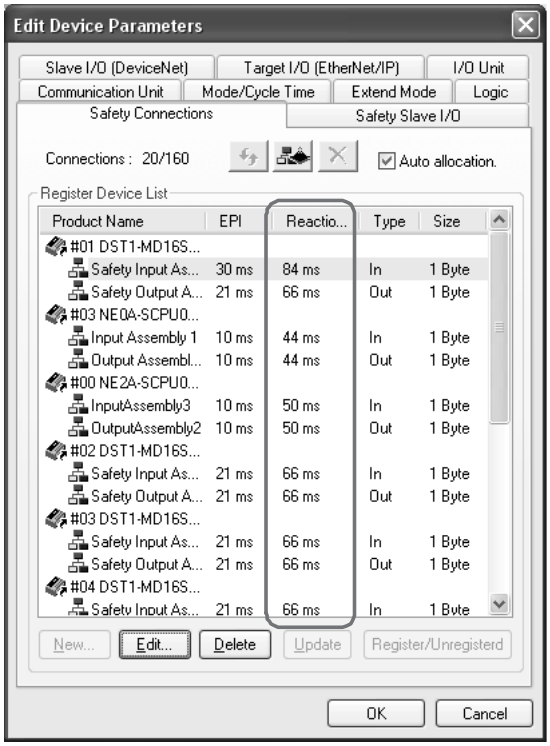
Checking the Network Reaction Time

The Network Configurator automatically calculates the Safety Connection network reaction time when the EPI is set.

Procedure

1,2,3...

1. Select the Target NE2A-series CPU Unit in the Network Configuration Pane.
2. Select ***Device - Parameter - Edit***.
   The Edit Device Parameters Dialog Box will be displayed.
3. Click the **Safety Connections** Tab in the Edit Device Parameters Dialog Box and check the Reaction Time.



Checking the Reaction Time

Check that the calculated reaction times for all safety chains satisfy the required specifications as outlined in *8-2-2 Calculating the Reaction Time*.

⚠ WARNING

Serious injury may possibly occur due to loss of required safety functions. Always confirm that the reaction time calculated for each safety chain satisfies the required specifications.



Improving the Reaction Time

If there is a Safety Connection with a reaction time that exceeds the required specifications, re-examine the network design, taking into consideration the following points for the reaction time to meet the required specifications

- Shortening the EPI will shorten the network response time. Shortening the EPI, however, narrows the bandwidth that can be used for other connections.
- When a DeviceNet network is being used, the baud rate can be accelerated. Take note of the maximum length of the network and the type of cable.

13-5 Standard I/O Communications Network Response Performance

The Network Configurator checks the following values and calculates the Standard I/O Communications response performance.

- NE2A-series Controller Instruction Execution Cycle Time
- NE2A-series Controller Peripheral Servicing Cycle Time
- DeviceNet Standard I/O Communications cycle time
- EtherNet/IP Tag Data Link RPI

Checking the Network Response Performance

Check the network response performance of the DeviceNet Standard I/O Communications and EtherNet/IP Tag Data Link based on the formulas and calculation examples in *8-2-2 Calculating the Reaction Time*.

Improving the Network Response Performance

If the network response performance exceeds the required specifications, re-examine the network design, taking into consideration the following points so that it satisfies the required specifications.

- Shortening the communications cycle time will shorten the network response time. Shortening the communications cycle time, however, narrows the bandwidth that can be used for other connections.
- When a DeviceNet network is being used, the baud rate can be accelerated. Take note of the maximum length of the network and the type of cable.

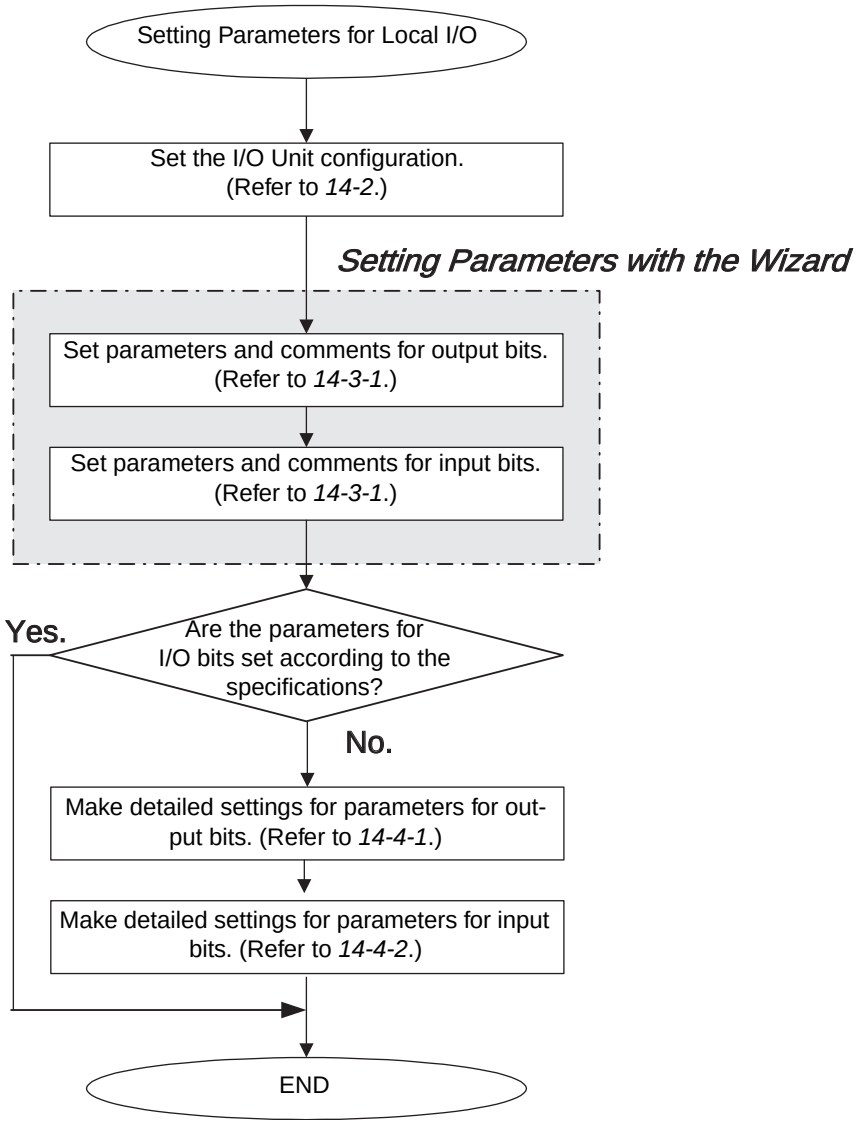
SECTION 14
Setting Parameters for Local I/O

This section describes how to set parameters for local I/O.

14-1 Overall Procedure 332
14-2 Setting the I/O Unit Configuration 333
14-2-1 Setting I/O Units 333
14-2-2 Copying I/O Units 334
14-3 Setting the I/O Configuration from the Wizard 336
14-3-1 Setting the Parameters for Safety I/O Bits 336
14-4 Setting the I/O Configuration of Individual I/O Bits 342
14-4-1 Setting Safety Output Bits 342
14-4-2 Setting Safety Input Bits 345

14-1 Overall Procedure

This section describes the configuration of Safety I/O Units (I/O Units) used to connect Safety Devices to NE2A-series Controllers, and how to set parameters for local I/O bit. The overall procedure for setting parameters for local I/O is as follows:



14-2 Setting the I/O Unit Configuration

You can design the configuration of I/O Units of an NE2A-series Controller to which I/O devices are connected. The required I/O Unit configuration is determined from the types of the I/O devices and the specifications required by the safety category of the equipment.

14-2-1 Setting I/O Units

You can set the configuration of I/O Units connected to an NE2A-series CPU Unit.

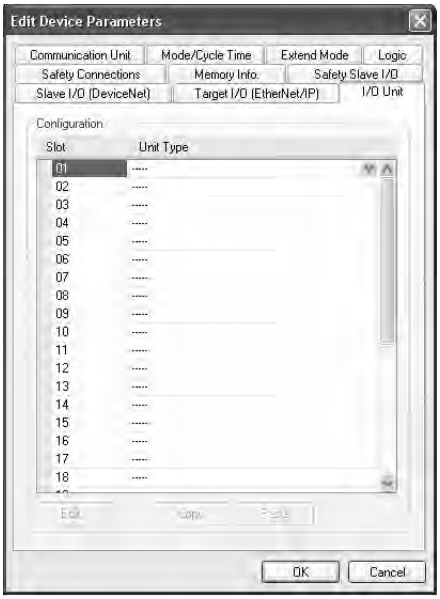
Making the Settings from the Network Configurator

Procedure

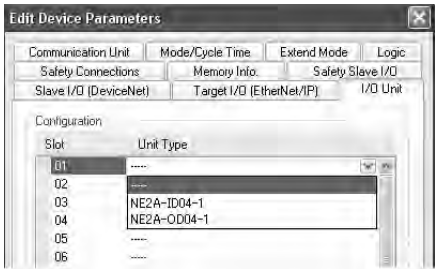
1,2,3... 1. In the Network Configuration Pane, select the NE2A-SCPU01 CPU Unit to set.

2. Select ***Parameters - Edit*** from the Device Menu.
   The Edit Device Parameters Dialog Box will be displayed.

3. Click the **I/O Unit** Tab.
   The I/O Unit Tab Page will be displayed.



4. Set the slot and Unit type.



The settings for the Unit Type Field are described in the following table:

Unit type	Description
NE2A-ID04-1	Safety Input Unit
NE2A-OD04-1	Safety Output Unit

Note (a) The slot number is allocated in numerical order from 01 starting from the Unit to the right side of the CPU Unit.

(b) To delete a Unit that is already set, select "----" from the list of Unit types.

5. Set the Unit type for all slots of the I/O Units in the NE2A-series Controller.
6. Click the **OK** Button.
   The Edit Device Parameters Dialog Box will close.

When you exit the Edit Device Parameters Dialog Box, the Units that were registered will be shown in the I/O Tag List.

Making the Settings from the Logic Editor

Procedure

1,2,3...

1. Select ***Settings - I/O Unit Configuration*** from the Device Menu.
   The I/O Unit Tab Page will be displayed in the dialog box showing the Unit settings.
2. Specify the slot and Unit in the same way as for the Network Configurator procedure.
3. Set the Unit type for all slots of the I/O Units in the NE2A-series Controller.
4. Click the **OK** Button
   The Edit Device Parameters Dialog Box will close.

When you exit the Edit Device Parameters Dialog Box, the Units that were registered will be shown in the I/O Tag List.

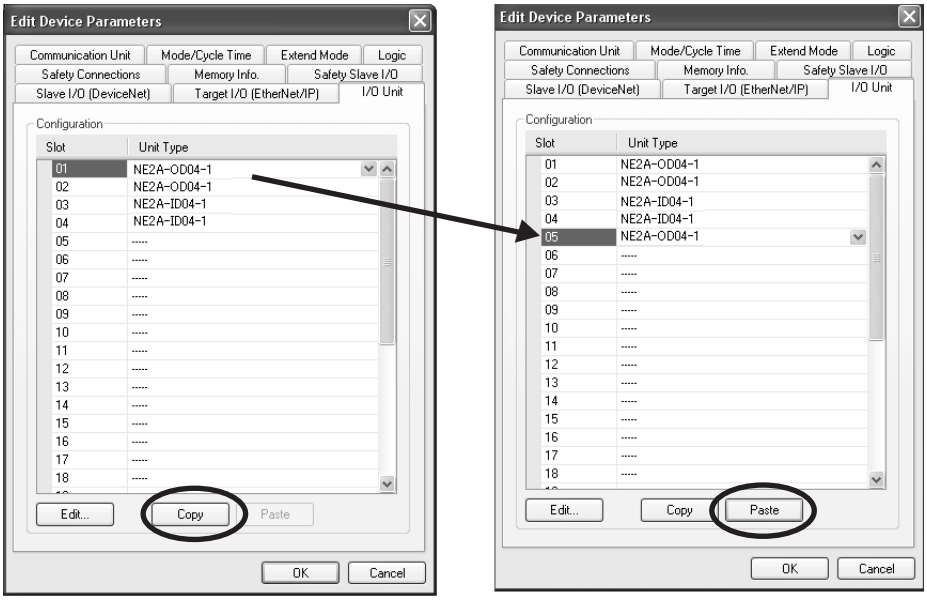
14-2-2 Copying I/O Units

An I/O Unit for which the parameters for I/O bits have already been set using the procedures in *14-3 Setting the I/O Configuration from the Wizard* and *14-4 Setting the I/O Configuration of Individual I/O Bits* can be copied. This helps increase efficiency when setting the same Safety Device configuration for more than one I/O Unit.

Procedure

1,2,3...

1. In the I/O Unit Tab Page of the Edit Device Parameters Dialog Box, select the slot of the I/O Unit to be copied, and then click the **Copy** Button.
2. Select the slot where the I/O Unit copy is to be created and click the **Paste** Button.
   If you select a slot that has already been set, a message box will be displayed to allow you to confirm overwriting.


Edit Device Parameters
Communication Unit
Mode/Cycle Time
Extend Mode
Logic
Safety Connections
Memory Info.
Safety Slave I/O
Slave I/O (DeviceNet)
Target I/O (EtherNet/IP)
I/O Unit
Configuration
Slot
Unit Type
01 NE2A-OD04-1
02 NE2A-OD04-1
03 NE2A-ID04-1
04 NE2A-ID04-1
05 -----
06 -----
07 -----
08 -----
09 -----
10 -----
11 -----
12 -----
13 -----
14 -----
15 -----
16 -----
17 -----
18 -----
Edit...
Copy
Paste
OK
Cancel
Edit Device Parameters
Communication Unit
Mode/Cycle Time
Extend Mode
Logic
Safety Connections
Memory Info.
Safety Slave I/O
Slave I/O (DeviceNet)
Target I/O (EtherNet/IP)
I/O Unit
Configuration
Slot
Unit Type
01 NE2A-OD04-1
02 NE2A-OD04-1
03 NE2A-ID04-1
04 NE2A-ID04-1
05 NE2A-OD04-1
06 -----
07 -----
08 -----
09 -----
10 -----
11 -----
12 -----
13 -----
14 -----
15 -----
16 -----
17 -----
18 -----
Edit...
Copy
Paste
OK
Cancel

14-3 Setting the I/O Configuration from the Wizard

The parameters of the I/O bits of an I/O Unit in an NE2A-series Controller be set using a wizard.

14-3-1 Setting the Parameters for Safety I/O Bits

The steps for setting parameters with the wizard are as follows:

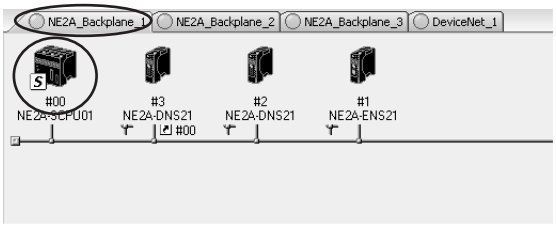


Step	Settings
Edit Output Bits	Set the types of devices and comments for the devices to connect to the output bits.
Edit Input Bits	Set the types of devices and comments for the devices to connect to the input bits.
Confirm Configuration	Check the settings.

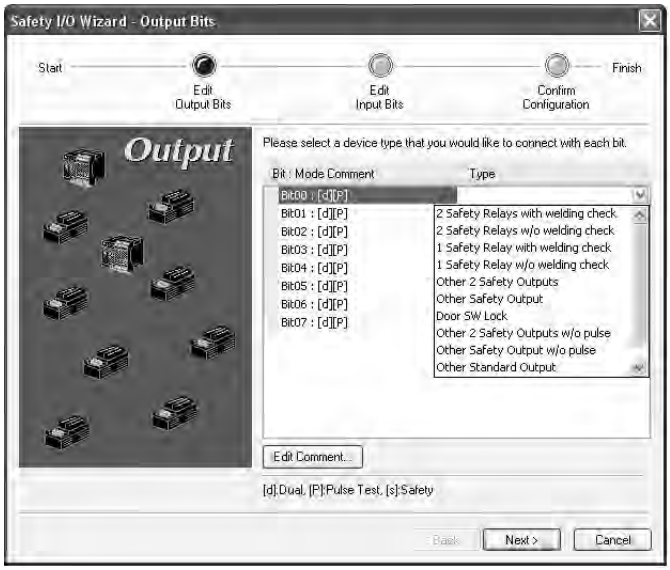
Note If either a Safety Output Unit or Safety Input Unit has been specified, only the step for setting the bits of the specified Unit will be displayed. If no I/O Unit has been specified, the above steps will not be displayed, and it will not be possible to set parameters with the wizard.

Procedure

1,2,3... 1. In the Network Configuration Pane, select the NE2A-SCPU01 CPU Unit to set.



2. Select ***Parameters - Wizard*** from the Device Menu.
The following dialog box will be displayed.



Note The number of output bits depends on the number of Output Units that is set. (Number of bits = Number of Output Units × 4)

3. In the Safety I/O Wizard - Output Bits Dialog Box, specify the type of device to connect to each output bit. You can specify any of the following types.

Type	Contents
2 Safety Relays with welding check (*1)	Used to connect two safety relay outputs and perform a welding check.
2 Safety Relays w/o welding check (*1)	Used to connect two safety relay outputs but no perform a welding check.
1 Safety Relay with welding check	Used to connect one safety relay output and perform a welding check.
1 Safety Relay w/o welding check	Used to connect one safety relay output but no perform a welding check.
Other 2 Safety Outputs (*1)	Used to connect two outputs without welding check.
Other Safety Output	Used to connect one output without welding check.
Door SW Lock	Used to connect an electromagnetic door switch.
Other 2 Safety Outputs w/o pulse (*1)	Used to connect two outputs that do not require a check pulse.
Other Safety Output w/o pulse	Used to connect an output that does not require a check pulse.
Other Standard Output	Used for Standard Outputs.
Not Use	The output is not used.

*1 This device type can be selected only when the bit number is an even number.

- If you select a device type for which the welding check is specified in the bit settings, the following dialog box will be displayed.

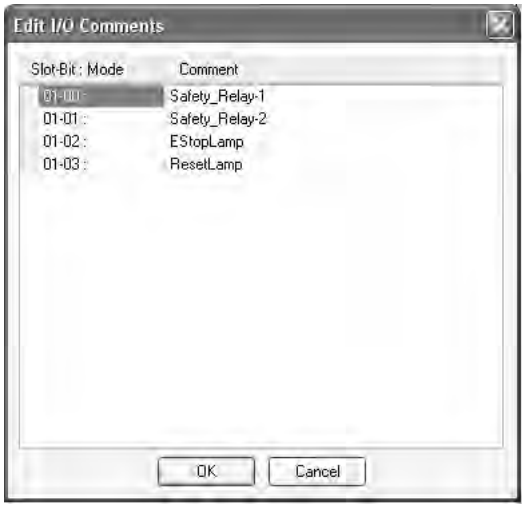


In this dialog box, set the input bit for which the welding check (feedback input) is to be performed and click the **OK** Button.

Note The number of the output bit for which a welding check is specified corresponds to the numeric value within parentheses in “Feedback (01-00)” that is displayed in the Safety I/O Wizard - Input Bits Dialog Box.

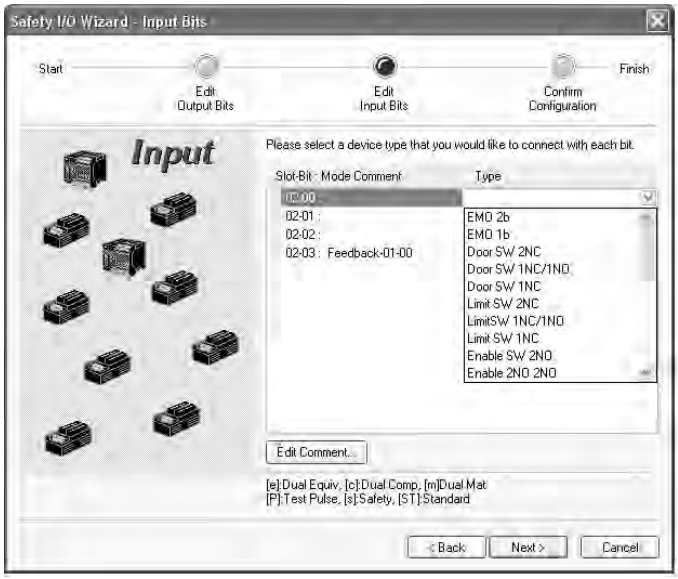
4. Make the settings for the other output bits.

5. Click the **Edit Comment** Button to edit the comments of output bits in the Edit I/O Comments Dialog Box.



The comments set in this dialog box are used as I/O tags in the Logic Editor.

6. Edit the comments for the output bits, and then click the **OK** Button.
7. Click the **Next** Button in the Safety I/O Wizard - Output Bits Dialog Box. The dialog box displaying the settings of input bits will be displayed.



Note The number of input bits depends on the number of Input Units that is set. (Number of bits = Number of Input Units × 4)

8. In the Safety I/O Wizard - Input Bits Dialog Box, specify the type of the device to connect to each input bit. You can specify any of the following types.

Device type	Description
EMO 2b (*1)	Used to connect two inputs from the Emergency Stop Button.
EMO 1b	Used for one input from the Emergency Stop Button.
Door SW 2NC (*1)	Used for two NC contact inputs from a door switch.
Door SW 1NC/1NO (*1)	Used for one NC and one NO contact input from a door switch.
Door SW 1 NC	Used for one input from a door switch.
Limit SW 2NC (*1)	Used for two NC contact inputs from a limit switch.
Limit SW 1NC/1NO (*1)	Used for one NC and one NO contact input from a limit switch.
Limit SW 1 NC	Used for one input from a limit switch.
Enable SW 2NO (*1)	Used for two inputs from an enabling switch.
Enable 2NO/1NC/1NC (*2)	Used for four inputs from an enabling switch.
Two Hand Switch (*1)	Used for two inputs from a two hand switch.
Other 2NC (*1)	Used for two NC contact inputs other than the above.
Other 2 NO (*1)	Used for two NO contact inputs other than the above.
Other 1NC/1NO (*1)	Used for one NC and one NO contact input other than the above.
Other 1NO/1NC (*1)	Used for one NO and one NC contact input other than the above.
Other 1 NC (Single Contact)	Used for a contact input other than the above.
SLC 2 outputs (*1)	Used for two inputs from a light curtain.
SLC 1 output	Used for one input from a light curtain.
Other PNP 2 outputs (*1)	Used for two inputs from a semiconductor.
Other PNP 1 output	Used for one input from a semiconductor.
Reset SW	Used for input from reset switch.
Feed back (EDM Input)	Used for EDM feedback signal.
Mechanical Contact	Used for one input from a mechanical contact.
Single Beam Safety Sensor	Used for one input from a Single-beam Safety Sensor.
Noncontact Switch D40A (*1)	Used for two inputs from a non-contact switch.
Safety Mat (*1)	Used for two inputs from a safety mat.
Standard SW	Used for an input from a general-purpose switch.
Not Use	The input is not used.

*1 This device type can be selected only when the bit number is an even number.

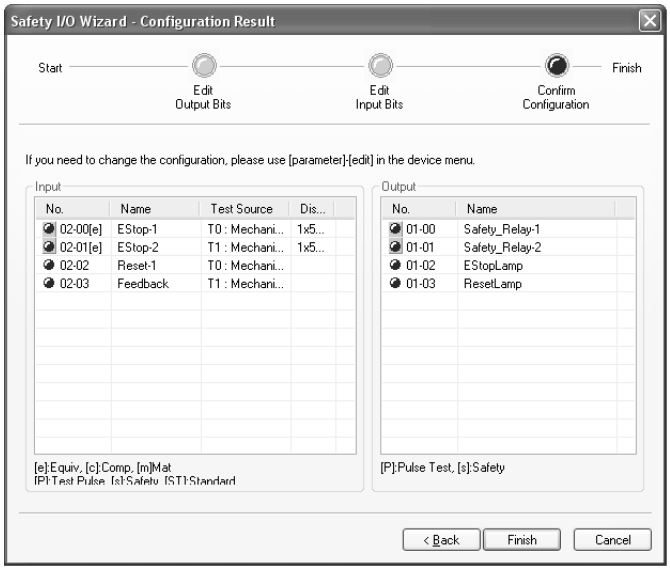
*2 This device type can be selected only when the bit number is an even number and only when four or more bits are remaining.

9. Make the settings for the other input bits.
10. Click the **Edit Comment** Button to edit the comments for input bits in the Edit I/O Comments Dialog Box.



The comments set in this dialog box are used as I/O tags in the Logic Editor.

11. Edit the comments for the input bits, and then click the **OK** Button.
12. Click the **Next** Button in the Safety I/O Wizard - Input Bits Dialog Box.
    A dialog box showing the list of settings configured with the wizard will be displayed.



The following settings are displayed.

Item	Settings
Test Source	A pulse is output from the test output bit to diagnose the Safety Devices. The pulse is output at different times from the output bits: test output 0 and test output 1.
Discrepancy Time	For two inputs set in a Dual Channel Mode, the time is monitored from a change in the value of one input to a change in the value of the other input. This is called the discrepancy time.

The meanings of symbols used for with I/O bit number are described in the following table:

Input Mode	Symbol	Dual channel channel mode	Symbol
Not Used	N	Single Channel	None
Test pulse from test output	P	Dual Channel Equivalent	e

Input Mode	Symbol	Dual channel channel mode	Symbol
Used as Safety Input	S	Dual Channel Complementary	c
Used as standard input	ST	---	---

Output Mode	Symbol	Dual channel channel mode	Symbol
Not Used	N	Single Channel	None
Safety	S	Dual Channel	d
Safety Pulse Test	P	---	---

13. Check the settings, and then click the **Finish** Button.

This completes the setting of I/O bits with the wizard. Refer to *14-4 Setting the I/O Configuration of Individual I/O Bits*, for details on changing the test source (test bit) or discrepancy time, and setting the maintenance parameters.

14-4 Setting the I/O Configuration of Individual I/O Bits

Although the Safety I/O bits can be set easily with the wizard, this section describes how to make detailed settings for the Safety I/O bits. The parameters for the Safety I/O bits are set according to the type of Safety Device that is connected to the I/O Unit.

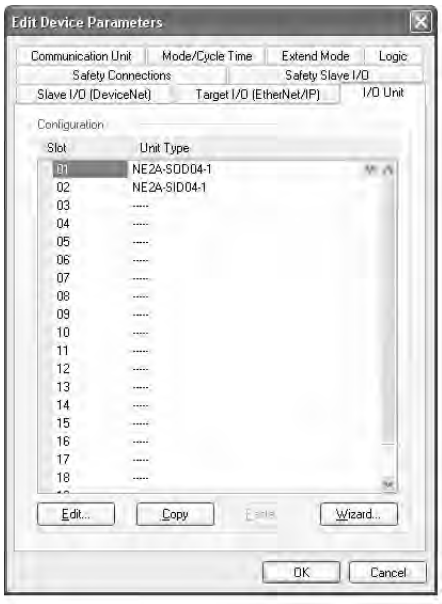
14-4-1 Setting Safety Output Bits

You can set the error latch time for the Safety Output Unit and you can set parameters for individual bits in the Local Output Dialog Box displayed from the I/O Unit Tab Page.

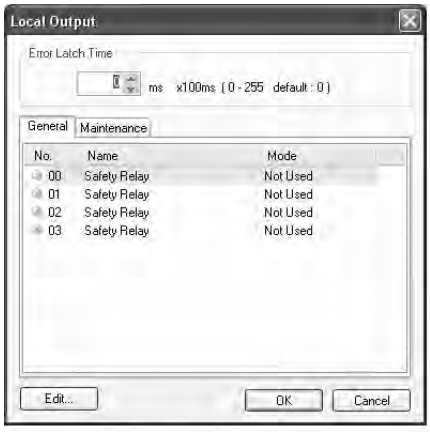
Procedure

1,2,3...

1. In the Network Configuration Pane, select the NE2A-SCPU01 CPU Unit to set.
2. Select ***Parameters - Edit*** from the Device Menu.
   The Edit Device Parameters Dialog Box will be displayed.
3. Click the **I/O Unit** Tab.
   The I/O Unit Tab Page will be displayed.



4. In the *Slot* column of the tab page, select the slot of the Output Unit to set, and then click the **Edit** Button.
   The Local Output Dialog Box will be displayed.



Error Latch Time

The setting of the error latch time is described in the following table:

Set value	Description	Default
0 to 255 (× 100 ms)	You can set the time to latch the error state when an error occurs in a bit of the Safety Output Unit. The error state will continue until the error latch time passes even if the cause of the error is removed. Duration of error latch time: 0 to 25,500 ms	0 (ms)

Setting the Parameters for Individual Bits

The details of the parameters displayed by clicking the tabs are described in the following table:

Tab	Item	Description
General	I/O Comment	Displays the comments for the bit.
	Channel Mode	Displays the operation of the bit.
Maintenance	Monitor Mode	Displays the monitor value for the number of bit operations (fixed).
	Value	Displays the current number of bit operations.

Setting the Channel Mode (Edit Local Output Terminal Dialog Box)

1,2,3... 1. Click the **General** Tab in the Local Output Dialog Box.

2. Select the bit number to set, and then click the **Edit** Button.
The Edit Local Output Terminal Dialog Box will be displayed.



3. Set the I/O comment, channel mode, and dual channel channel mode. The settings are described in the following table:

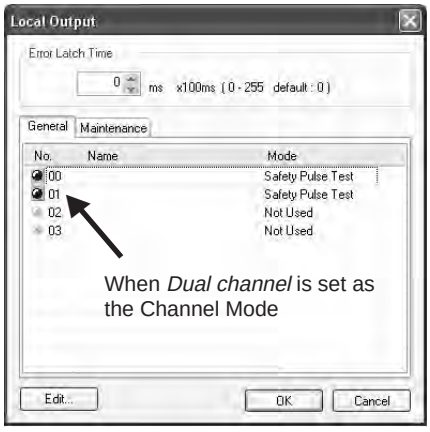
Item	Set value	Description	Default
I/O Comment	None	Set an I/O comment for the Safety Output bit. The I/O comment specified here is used as an I/O tag in the Logic Editor. Up to 48 characters can be specified. The characters that can be input are the same as those that can be input for variables. Refer to *Variable Specifications* on page 80.	None
Channel Mode	Not Used	Select when no output device is connected.	Not Used
	Safety	No test pulse is output when the output is ON. It is possible to detect contact with the positive output signal power supply line when the output is OFF, and to detect ground faults.	
	Safety Pulse Test	A test pulse is output when the output is ON. It is possible to detect contact with the positive output signal power supply line when the output is OFF or ON, to detect ground faults, and to detect short-circuits between output signals.	
Dual Channel Channel Mode	Single channel	Specifies using the bit as an independent Safety Output bit. If you set the dual channel channel mode to Single Channel, even paired Safety Output bits set to a Dual Channel Mode will be set to Single Channel Mode.	Single channel
	Dual channel	Specifies using Dual Channel outputs with paired Safety Output bits. The output will be ON if both bits of the paired Safety Output are normal.	

4. Click the **OK** Button.

Setting the Parameters for Paired Bits

In a Dual Channel Mode, bits 00 and 01 and bits 02 and 03 can be set as pairs.

- If you set one bit to a Dual Channel Mode, the other bit will also be set to the Dual Channel Mode.
- If a pair of bits is set to a Dual Channel Mode and you change the channel mode of one bit to Single Channel Mode, the other bit will also change to Single Channel Mode.
- If you set a Dual Channel Mode and then change the channel mode of one bit to *Not Used*, the other bit will change to *Single Channel Mode*.



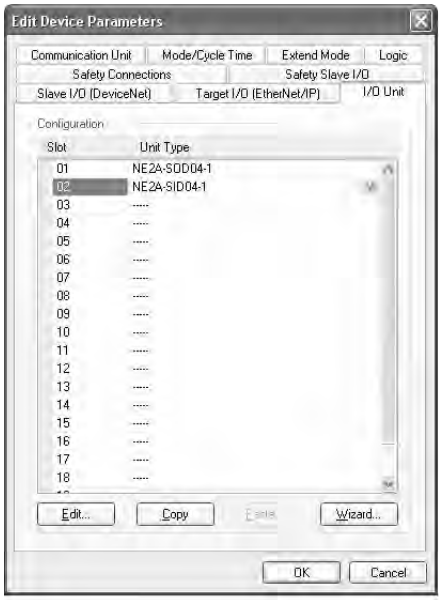
14-4-2 Setting Safety Input Bits

You can set a error latch time an Input Unit and you can set parameters for individual bits in the Local Input/Test Output Dialog Box displayed from the I/O Unit Tab Page.

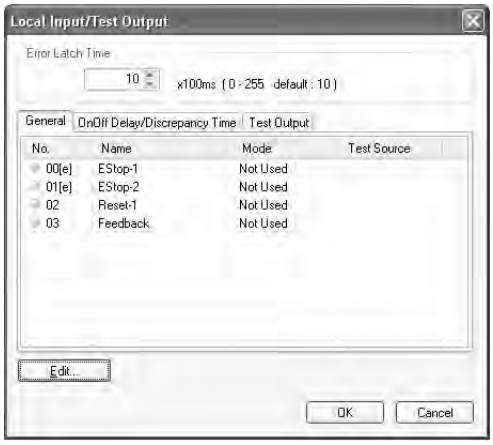
Procedure

1,2,3...

1. In the Network Configuration Pane, select the NE2A-SCPU01 CPU Unit to set.
2. Select ***Parameters - Edit*** from the Device Menu.
   The Edit Device Parameters Dialog Box will be displayed.
3. Click the **I/O Unit** Tab.
   The I/O Unit Tab Page will be displayed.



4. In the *Slot* column of the tab page, select the slot of the Input Unit to set, and then click the **Edit** Button.
   The Local Input/Test Output Dialog Box will be displayed.



Error Latch Time

The setting of the error latch time is described in the following table:

Set value	Contents	Default
0 to 255 (× 100 ms)	You can set the time to latch the error state when an error occurs in a bit of the Safety Input Unit. The error state will continue until the error latch time passes even if the cause of the error is removed. Duration of error latch time: 0 to 25500 ms	1000 (ms)

Setting the Parameters of Individual Bits

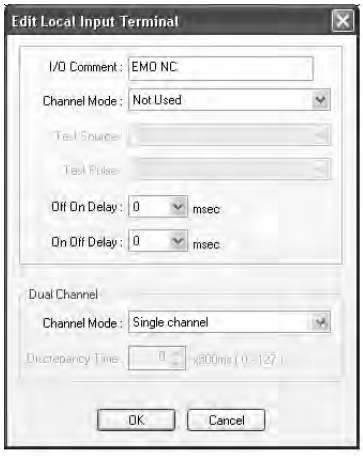
The details of the parameters displayed by clicking the tabs are described in the following table:

Tab	Item	Contents
General	I/O Comment	Displays the comment for the bit.
	Channel Mode	Displays the operation of the bit.
	Test Source	Displays the test bit.
OnOff Delay/ Discrep- ancy Time	ON Delay	Displays the ON Delay time.
	OF Delay	Displays the OFF Delay time.
	Discrepancy Time	Displays the Discrepancy time.
Test Output	Channel Mode	Displays the mode of the test bit.
	Test Pulse	Displays the pulse for an externally connected device.

Setting the Channel Mode

1,2,3... 1. Select either the **General** Tab or the **OnOff Delay/Discrepancy Time** Tab in the Local Input/Test Output Dialog Box.

2. Select the bit number to set, and then click the **Edit** Button.
   The Edit Local Input Terminal Dialog Box will be displayed.



3. Select and enter all parameters.
   The settings are described in the following table:

Item	Set value	Contents	Default
I/O Comment	None	Set the I/O comment for the Safety Input bit. The I/O comment specified here is used as an I/O tag in the Logic Editor. Up to 48 characters can be specified. The characters that can be input are the same as those that can be input for variables. Refer to *Variable Specifications* on page 80.	None
Channel Mode	Not Used	Specifies that no external device is connected.	Not Used
	Used as standard Input	Used when connecting a non-safety device.	
	Used as Safety Input	Used when connecting a Safety Device with a semiconductor output, such as a light curtain.	
	Test pulse from test out	Different Safety Devices can be connected by adding test outputs. The test output mode to be used in the test source is selected according to the Safety Device that is connected. It is possible to detect contact with the positive input signal power supply line and to detect short-circuits between other input signal lines.	
Test Source	Test Output 0 Test Output 1	When the channel mode of the Safety Input bit is set to *Test pulse from test out*, the test output bit to be used can be selected in combination with a Safety Input bit. **Note** When a Dual Channel Mode is set, the test output must be set for each bit of the pair.	Test Output0
Test Pulse	Mechanical contact	Specifies that a mechanical contact device is connected. The test output signal (pulse output) of the Safety Input Unit is input via the mechanical contact device. It is possible to detect contact with the positive input signal power supply line, to detect ground faults, and to detect short-circuits between other input signal lines.	Mechanical contact
	Single-beam Safety Sensor	Used when connecting a Single-beam Safety Sensor. A test signal is output for Single-beam Safety Sensor diagnosis.	
	Non-contact switch D40A	Specifies that the OMRON D40A Non-contact Door Switch is connected. A test signal is output for the D40A.	
	MAT	Specifies that a safety mat is connected. A test signal is output to diagnose the safety mat.	
ON Delay	0 - 1024 ms (selected)	Specifies the ON delay time.	0 ms

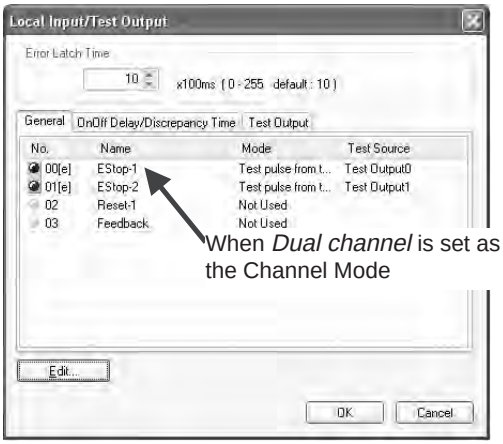
Item		Set value	Contents	Default
OFF Delay		0 - 1024 ms (selected)	Specifies the OFF delay time.	0 ms
Dual Channel	**Channel Mode**	Single channel	Specifies using the bit as an independent Safety Input bit.	Single channel
		Dual channel equivalent	Specifies using the bit as a dual channel equivalent input with paired Safety Input bits.	
		Dual channel complementary	Used as a dual channel complementary input with paired Safety Input bits.	
		MAT	The paired Safety Input bits can be used for a safety mat. This item can be set only in bits 00 and 01.	
	Discrepancy Time	0 - 127 (× 500 ms)	For two inputs set in a Dual Channel Mode, the time is monitored from a change in the value of one input to a change in the value of the other input. This is called the discrepancy time. When the value of the other input does not change within the set discrepancy time, an error will occur. Monitoring is disabled if 0 is set as the value.	500 ms

4. Click the **OK** Button.

Setting the Parameters for Paired Bits

In a Dual Channel Mode, bits 00 and 01, and bits 02 and 03 can be set as pairs.

- If you set one bit to a Dual Channel Mode, the other bit will also be set to the Dual Channel Mode.
- If a pair of bits is set to Dual Channel Mode and you change the channel mode of one bit to *Single Channel Mode*, the other bit will also change to Single Channel Mode.
- If you set a Dual Channel Mode and then change the channel mode of one bit to *Not Used*, the other bit will change to Single Channel Mode.



Restrictions When Setting Parameters

There are restriction in the parameter setting for some settings of the channel mode and dual channel channel mode. These restriction are described in the following table.

Channel mode	Dual channel channel mode	Test source	Test pulse
• Not Used • Used as standard input • Used as Safety Input	• Single channel • Dual channel equivalent • Dual channel complementary (See note.)	Cannot be set.	Cannot be set.
• Test pulse from test out	• Single channel	Test Output 0 Test Output 1	• Mechanical contacts • SIngle-beam Safety Sensor
	• Dual channel equivalent	Test Output 0 Test Output 1	• Mechanical contacts • D40A Non-contact Switch
	• Dual channel complementary	Test Output 0 Test Output 1	• Mechanical contacts
	• MAT	Test Output 0 (See note.)	• MAT

Note The following restrictions exist on setting MAT (i.e., when MAT is set for the dual channel channel mode).

- The channel mode is automatically set to *Test pulse from test out*.
- The Test Source must be *Test Output 0* (*Test Output 0* is set in the Test Source of bit 00, and *Test Output 1* is set in the Test Source of bit 01).
- A Test Source cannot be used for bit 02 or 03.

Note When input terminals are used in pairs, set the Dual Channel Mode to *Dual Channel*. This will make it easier to isolate errors because the relevant I/O indicators on the NE2A-ID04-1 will light red or go out if an error is detected for the input terminals.

SECTION 15
Creating Programs

This section describes how to program a NE2A-series Safety Network Controller.

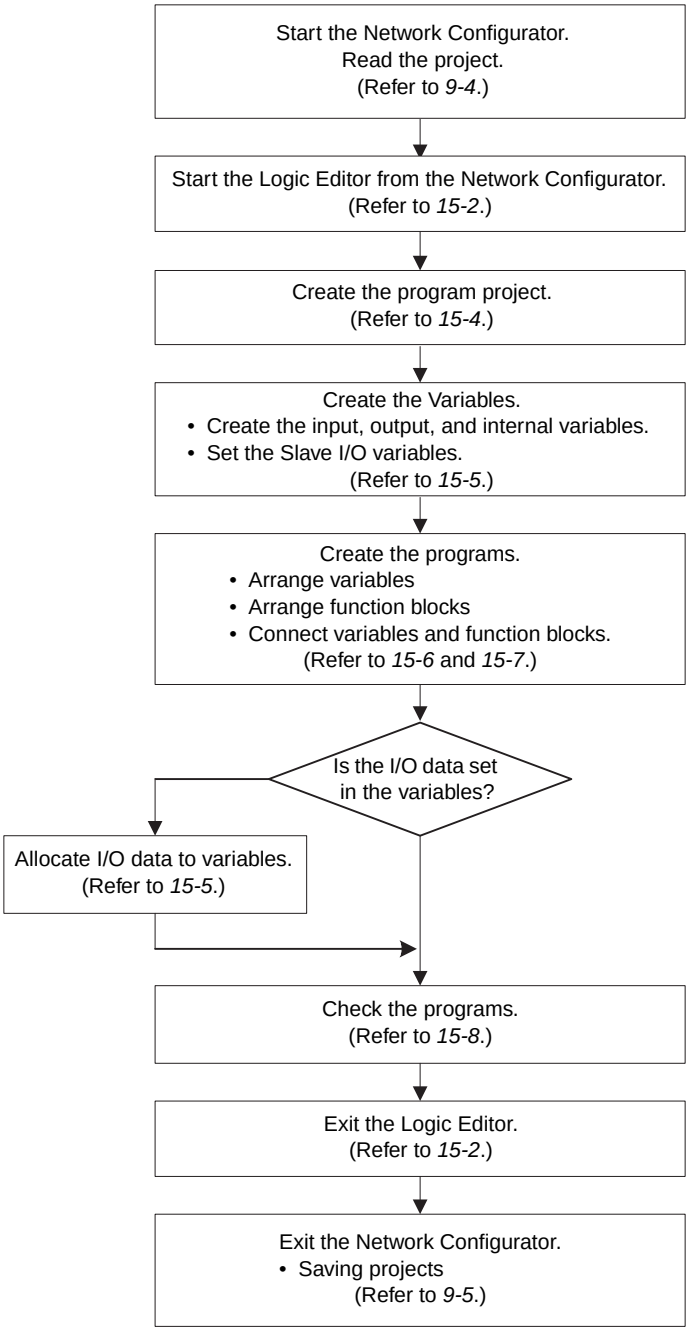
15-1 Overall Programming Procedure 352
15-2 Starting and Exiting the Logic Editor 353
15-3 Logic Editor Functions 354
15-3-1 Layout of the Logic Editor Windows 354
15-3-2 Logic Editor Menus 355
15-3-3 Using the Shortcut Keys in the Logic Editor 361
15-4 Creating Program Projects 364
15-4-1 Creating Program Projects 364
15-4-2 Setting Information in Projects 364
15-5 Creating Variables 366
15-5-1 Creating and Editing Variables 366
15-5-2 Exporting and Importing Variables 371
15-5-3 Finding and Replacing Variables 373
15-6 Creating Programs 376
15-6-1 Arranging Input Variables 376
15-6-2 Arranging Function Blocks 378
15-6-3 Function Block Settings 379
15-6-4 Arranging Output Variables 381
15-6-5 Arranging Internal Variables 381
15-6-6 Connecting Function Block Input/Output Signals 382
15-6-7 Arranging Text Boxes 383
15-7 Creating Sections 385
15-7-1 Creating Sections 385
15-8 Checking Programs 389
15-8-1 Checking Programs for Syntax Errors 389
15-8-2 Displaying the Variable Reference Report 390
15-8-3 Searching 391
15-9 Creating and Reusing Program Objects 393
15-9-1 Creating User-defined Function Blocks 394
15-9-2 Creating Program Objects 397
15-9-3 Reusing Programming 398
15-9-4 Importing NE1A-series Programs 400
15-10 Printing 402
15-10-1 Printing 402
15-10-2 Print Preview 403
15-10-3 Page Setup 404
15-10-4 Printer Settings 404

15-1 Overall Programming Procedure

This section describes the overall procedure for creating safety control logic using the Logic Editor.

Overall Programming Procedure

The following diagram shows the steps that are necessary to program an NE2A-series Controller.



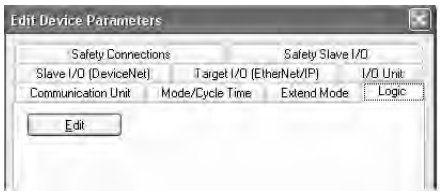
15-2 Starting and Exiting the Logic Editor

With the NEA2-series Controller, programs are created by using the Logic Editor. The Logic Editor is started from the Network Configurator.

Starting the Logic Editor

Procedure

1,2,3... 1. Double-click *NE2A-SCPU01* in the Network Configurator, or select the NE2A-SCPU01 and then select ***Parameter - Edit*** from the Device Menu. The Edit Device Parameters Window will be displayed.



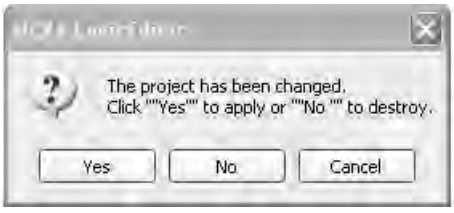
2. Click the **Logic** Tab and then click the **Edit** Button.
   The Logic Editor will start.

Exiting the Logic Editor

Exit the Logic Editor.

Procedure

1,2,3... 1. Select ***Exit*** from the File Menu.
   If changes were made but not saved, a message box will be displayed asking whether you want to save the changes.



2. Click the **Yes** Button to save the project.
   Click the **No** Button to not save the project.
   The display will return to the Edit Device Parameters Window in the Network Configurator.

Note The program will not be saved simply by returning to the Edit Device Parameters Window. To save the program, select ***Save*** or ***Save As*** from the File Menu of the Network Configurator, or save the network configuration when closing the Network Configurator.

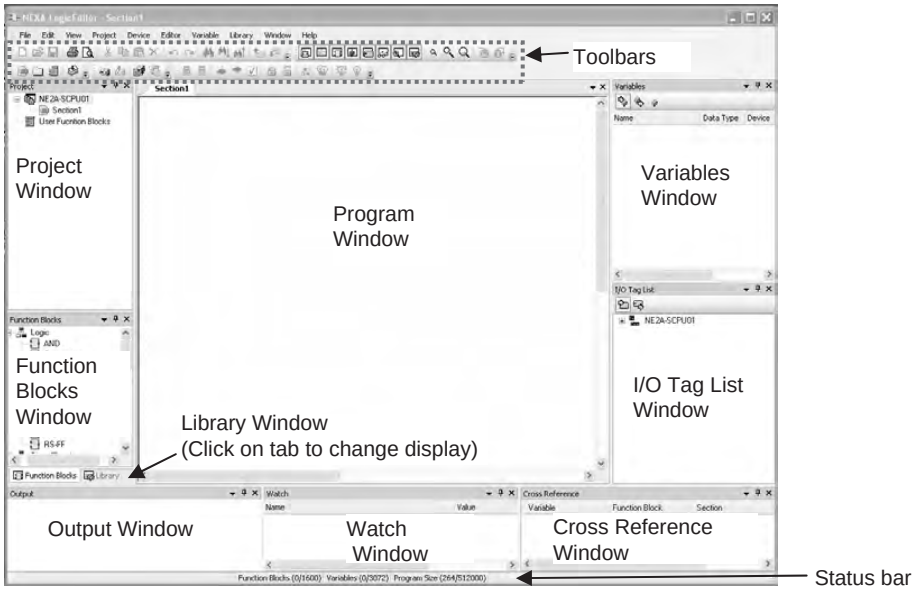
3. Click the **OK** Button in the Edit Device Parameters Window. The Logic Editor will be closed.

15-3 Logic Editor Functions

This section describes the windows, toolbars, and menu structure of the Logic Editor.
It also describes how to change between windows using shortcut keys.

15-3-1 Layout of the Logic Editor Windows

The Logic Editor consists of menus, windows, toolbars, and a status bar.



Windows

Window name	Description
Program Window	This window is for creating programs using function blocks.
Project Window	This window is for managing the entire project. It displays a list of sections and user-defined function blocks.
Function Blocks Window	This window is for managing safety function blocks.
Library Window	This window is for managing libraries. Libraries of user-defined function blocks and sections can be managed.
Variables Window	This window is for editing variables used in the program and displaying them in a list. There are pages for input variables, output variables, and internal variables.
I/O Tag List Window	This window displays a list of I/O tags for local I/O and remote I/O. The I/O tags can be used by allocating them to variables.
Output Window	This window displays the results when compiling or searching programs.
Watch Window	This window is for monitoring the input/output variables in online mode. Programs can be tested by force-setting and force-resetting variables.
Cross Reference Window	This window displays the cross references of selected variables. You can jump to the program by double-clicking on a variable displayed in this window.

Toolbars

Toolbar name	Description
Standard	Displays icons for the File Menu and the Edit Menu.
View	Displays icons for the View Menu.
Project	Displays icons for the Project Menu.
Variable	Displays icons for the Variable Menu.
Device	Displays icons for the Device Menu.

Status Bar

Item	Description
Function Blocks	Shows the total number function blocks and user-defined function blocks being used. The number of function blocks in use is displayed before the slash, which is followed by the maximum number of usable function blocks (1,600).
I/O Variables	Shows the number of I/O variables that have been created. The number of I/O variables that has been created is displayed before the slash, followed by the maximum number of usable variables (2,048).
Internal Variables	Shows the number of internal variables that have been created. The number of internal variables that have been created is displayed before the slash, followed by the maximum number of usable variables (1,024).
Program Size	Displays the program size in bytes. The current program size is displayed before the slash, which is followed by the maximum program size (512,000 bytes).

15-3-2 Logic Editor Menus

This section gives the names and purposes of the menu commands of the Logic Editor.

File Menu

Command		Description	Toolbar icon	Offline	Online
User Function Block	**Save**	Saves a user-defined function block that is being edited to a file.		OK	OK
	Read	Reads a user-defined function block from the system folder into the project.		OK	OK
	Import	Imports a user-defined function block file (".ufb) into the project.	---	OK	OK
	Export	Exports a user-defined user block as a file (".ufb).	---	OK	OK
Import	**NE1A Logic File**	Imports a program that was created for the NE1A and then exported (*.led file).	---	OK	OK
	NE1A Function Block	Imports a function block that was created for the NE1A and then exported (*.fbd file).	---	OK	OK
Print		Selects the program, variable list, function block settings, and other items to be printed. Sets the printer.		OK	OK
Print Preview		Displays the print contents on the screen.		OK	OK
Setup Page Size		Sets the page size and printing direction.	---	OK	OK
Print Settings		Edits the contents to be printed for the title, header, and footer.	---	OK	OK
Exit		Exits the Logic Editor.	---	OK	OK

Edit Menu

Command	Description	Toolbar icon	Offline	Online
Undo	Cancels the operation that was just executed. Up to 100 operations can be canceled.		OK	OK
Redo	Redoes an operation that has been undone.		OK	OK
Cut	Cuts the selected area. In the Program Window, all function blocks, variables, and connections (connected to the selected objects) within the selected area will be cut. In the Variable Window, the selected variables will be cut.		OK	OK
Copy	Copies the selected area. The items that are copied are the same as those that are cut for the Cut command.		OK	OK
Paste	Inserts copied or cut data to a selected location.		OK	OK
Delete	Deletes the selected area. The items that are deleted are the same as those that are cut for the Cut command. Sections selected in the Project Window can also be deleted.		OK	OK
Rename	Changes the project name, section name, folder name, or user-defined function block name.	---	OK	OK
Select All	Selects all items in the active window. In the Program Window, all objects will be selected. In the Variable Window, all variables will be selected. In the Watch Window, all registered variables will be selected.	---	OK	OK
Move Upward	Moves the selected section up in the Project Window. Moves the selected variable up in the Variable Window.		OK	OK
Move Downward	Moves the selected section down in the Project Window. Moves the selected variable down in the Variable Window.		OK	OK

Command	Description	Toolbar icon	Offline	Online
Find	Displays a search dialog box will be displayed. The following items can be searched for in the Program Window. • Function block names • Variable names • I/O names (terminal names) • Comments The following items can be searched for in the Variable Window. • Variable names • I/O names (terminal names)		OK	OK
Find Next	Moves to the next item that matches the search conditions.		OK	OK
Find Prev	Moves the previous item that matches the search conditions.		OK	OK
Replace	Replaces the item that matches the search conditions. The following items can be replaced in the Program Window. • Variable names • Function blocks The following items can be replaced in the Variable Window. • Variable names	---	OK	OK

View Menu

Command		Description	Toolbar icon	Offline	Online
Window	**Project**	Displays or hides the Project Window.		OK	OK
	Output	Displays or hides the Output Window.		OK	OK
	Function Blocks	Displays or hides the Function Blocks Window.		OK	OK
	Variables	Displays or hides the Variables Window.		OK	OK
	I/O Tag List	Displays or hides the I/O Tag List Window.		OK	OK
	Watch	Displays or hides the Watch Window.		OK	OK
	Library	Displays or hides the Library Window.		OK	OK
	Cross Reference	Displays or hides the Cross Reference Window.		OK	OK
	Program Chain	Displays a window that shows the program chain from a program output to a program input.		OK	OK
Toolbar	**Standard**	Displays or hides the Standard Toolbar.	---	OK	OK
	View	Displays or hides the View Toolbar.	---	OK	OK
	Project	Displays or hides the Project Toolbar.	---	OK	OK
	Variable	Displays or hides the Variable Toolbar.	---	OK	OK
	Device	Displays or hides the Device Toolbar.	---	OK	OK
Status Bar		Displays or hides the Status Bar.	---		OK

Command		Description	Toolbar icon	Offline	Online
Variable	**Input**	Changes the Variable Window to display input variables.	---	OK	OK
	Output	Changes the Variable Window to display output variables.	---	OK	OK
	Internal	Changes the Variable Window to display internal variables.	---	OK	OK
I/O Tag List	**Input**	Changes the displayed I/O tag list to input tags.	---	OK	OK
	Output	Changes the displayed I/O tag list to output tags.	---	OK	OK
Zoom In		Zooms in the Program Window.		OK	OK
Zoom Out		Zooms out of the Program Window.		OK	OK
Zoom to Fit		Adjusts the Program Window display to fit the width of the window.		OK	OK

Project Menu

Command		Description	Toolbar icon	Offline	Online
New	**Section**	Creates a new section.		OK	OK
	Folder	Creates a new folder.		OK	OK
	User Function Block	Creates a new user-defined function block.		OK	OK
Edit		Enables editing the selected section.	---	OK	OK
Build		Checks for syntax errors in the program.		OK	OK
Authentication		Authenticates the password for a user-defined function block with a password setting to enable accessing and editing the function block.	---	OK	OK
Change Password		Changes the password required to access and edit a user-defined function block.	---	OK	OK
Display Activation Key		Enables checking the activation key required to reuse user-defined function blocks from a library.	---	OK	OK
Property		Displays the properties of the project or a user-defined function block.	---	OK	OK

Device Menu

Command		Description	Toolbar icon	Offline	Online
Setup	**I/O Unit Setting**	Displays the I/O Unit settings screen.	---	OK	OK
	System Parameter	Displays the system settings dialog box.	---	OK	OK
	Slave I/O	Displays the screen for setting assembly data for Safety Slave I/O and Standard Slave I/O.	---	OK	OK
Change Mode		Switches between IDLE Mode and RUN Mode.	---	---	OK

Command		Description	Toolbar icon	Offline	Online
Force Mode	**Start**	Changes to Force Mode.		---	OK
	Stop	Changes from Force Mode to Normal Mode.		---	OK
	Force On	Turns ON the selected variable.		---	OK
	Force Off	Turns OFF the selected variable.		---	OK
	Force Release	Releases force-setting and force-resetting for the selected variables.	---	---	OK
	Force Release All	Releases all force-set and force-reset variables.	---	---	OK
	Upload Force List	Displays all variables that are force-set or force-reset in the Watch Window.	---	---	OK
Monitor		Starts or stops monitoring variables and function blocks.		---	OK

Editor Menu

Command		Description	Toolbar icon	Offline	Online
Insert	**Function Block**	Inserts a function blocks at the curser position.	---	OK	OK
	Variable	Inserts an input or output variable at the curser position.	---	OK	OK
	Text Box	Inserts a comment at the curser position.	---	OK	OK
Add to Watch Window		Registers the selected variables in the Watch Window.	---	OK	OK
Function Block Help		Displays help on the selected function block.	---	OK	OK
Properties		Displays the parameter settings of selected function blocks.	---	OK	OK

Variable Menu

Command		Description	Toolbar icon	Offline	Online
Add		Adds a new variable.		OK	OK
Edit		Edits the parameter settings for an existing variable. If the change affects the program, a warning will be displayed in a message window.		OK	OK
Changing Variable Usage	**Input**	Changes an output variable or internal variable to an input variable. If the change affects the program, a warning will be displayed in a message window.	---	OK	OK
	Output	Changes an input variable or an internal variable to an output variable. If the change affects the program, a warning will be displayed in a message window.	---	OK	OK
	Internal	Changes an input variable or an output variable to an internal variable. The actual I/O allocation will be canceled if a variable is changed to an internal variable. If the change affects the program, a warning will be displayed in a message window.	---	OK	OK
Import		Imports variables from an external CSV file.		OK	OK

Command		Description	Toolbar icon	Offline	Online
Export	**Export Variables**	Exports the current variable data into an external CSV-format file.		OK	OK
	Export Tags	Exports the current tag list into an external CSV-format file.		OK	OK
Create from I/O Tag List		Imports variables from the actual I/O list if the remote I/O connection is already set or the local I/O already exists. The I/O terminal names will be used as the variable names.	---	OK	OK
Add to Watch Window		Registers the selected variables to the Watch Window.	---	OK	OK
Variable Reference Report		Displays a list of the variables that are being used.	---	OK	OK
Jump		Jumps to a location in the program where the selected variable is used.	---	OK	OK
Report changes in variable assignments		If this check box is selected, any changes to variable assignments will be reported. When designing the system, enable reporting of changes in assignments to prevent unintended program operation caused by assignment changes. If changes will not be made to variable assignments, e.g., for maintenance, clear the selection of this check box to increase the speed of reading and uploading project files.	---	OK	OK

Library Menu

Command	Description	Toolbar icon	Offline	Online
Add to Project	Registers the section or user-defined function block that is selected in the Library Window in the library.	---	OK	OK
Add to Library	Registers the section or user-defined function block that is selected in the Project Window in the library.	---	OK	OK
Map Folder	Registers a folder for display in the Library Window.	---	OK	OK
Disconnect Folder	Deletes a folder from the library.	---	OK	OK
Refresh	Updates the Library Window display.	---	OK	OK
New Folder	Creates a folder.	---	OK	OK
Delete	Deletes the section or user-defined function block that is selected in the Library Window from the library.	---	OK	OK
Property	Edits the property information of the library file.	---	OK	OK

Window Menu

Command	Description		Toolbar icon	Offline	Online
Hide All	Hides all windows.		---	OK	OK
Close All	Closes all Program Windows.		---	OK	OK
Section	Shows the sections that are in the Program Window. (Sections being displayed will be checked.)		---	OK	OK
Window	OK	Closes the pane.	---	OK	OK
	Activate	Switches the section displayed in the Program Window to the selected section.			
	Close Window	Closes the selected section in the Program Window.			

Help Menu

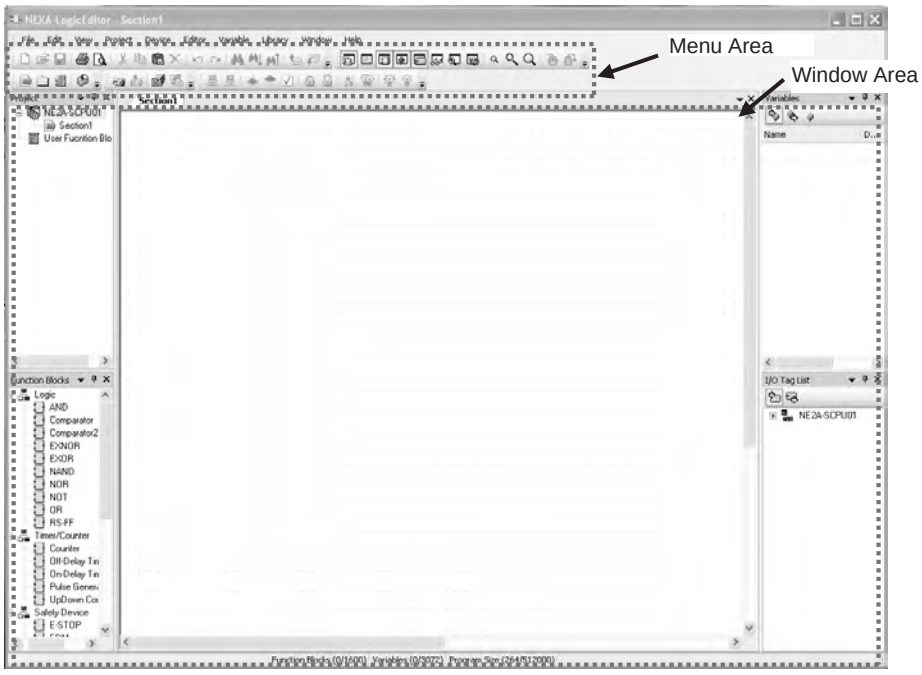
Command	Description	Toolbar icon	Offline	Online
Topic	Displays help on the selected function block.	---	OK	OK
About	Displays version information.	---	OK	OK

15-3-3 Using the Shortcut Keys in the Logic Editor

You can perform most operations with the shortcut keys in an NE2A-series Safety Network Controller. The details on operations performed with the shortcut keys in each window are described in different sections. This section describes how to select a menu or window.

Switching between Menus and Windows

Press the **F10** Key to switch from the Windows Area to the Menus Area, and press the **ESC** Key to switch from the Menus Area to the Windows Area. (When you switch to the Menus Areas, the File Menu will be selected.)

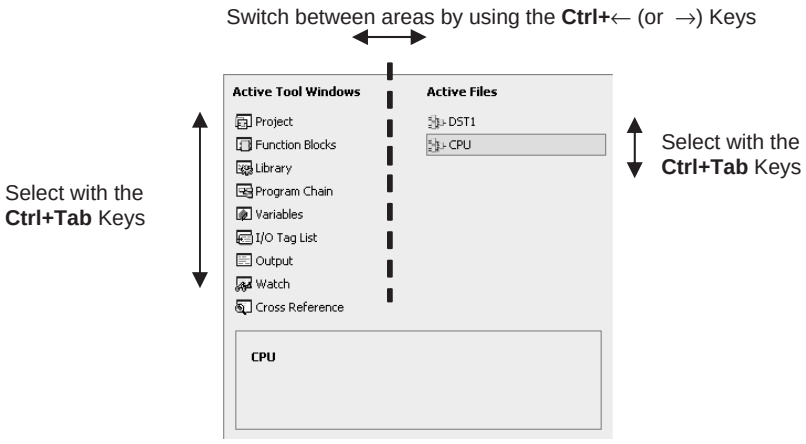


Selecting a Window or Section

Use the following procedure to switch between work windows and sections.

- To switch between active windows, press the **Ctrl+Tab** Keys. The window shown below will be displayed.
- If you keep the **Ctrl** Key pressed you can hold the display of the window shown below.
- If you press the **Ctrl+**← or **Ctrl+**→ Keys, you can switch between Active Tool Windows (group of windows) and Active Files (group of sections).
- Press the **Ctrl+Tab** Keys to switch between windows or between sections.
- When you release the **Ctrl** Key, you will be able to operate the shortcut keys in the window or section where the cursor is displayed.

The Active Tool Windows Area lists all the windows, while the Active Files Area lists the sections displayed in the Program Window Tag.



Example:

Use the following procedure if you want to switch from a section to perform an operation in the Variable Window.

1,2,3...

1. Press the **Ctrl+Tab** Keys.
2. Press the **Ctrl+**← Keys.
   The cursor will move to the icon of the Project Window in the Active Tool Windows Area.
3. Press the **Ctrl+Tab** Keys three times.
4. Once the cursor is on the Variable Window, release the **Ctrl+Tab** Keys.
   You will now be able to operate the shortcut keys in the Variable Window.

Switching Menus

You can switch between the menus and the toolbars by first pressing the F10 Key to set menu group operation and then pressing the **Ctrl+Tab** Keys. If you press the **Ctrl+Tab** Keys when the menus are selected, the first icon in the toolbar will be selected.



If the icons are displayed in the above pattern, you can move from (1) to (2) to (3) to (4) to (5) and back to (1) by pressing the **Ctrl+Tab** Keys.

Use the following procedure to select items when a menu is selected.

- You use the ← or → Key to move to different items in the menu.
- When the ↓ Key is pressed, the list of items of the menu is displayed, with the cursor on the first item.
- You can again use the ↑ or ↓ Keys to move the cursor to another item.
- If menu items are present in a lower level as well, you can display the list of items in the lower level by pressing either the → Key or **Enter** Key.
- If there are no lower levels and you press the **Enter** Key on an item, the operation for that item will be executed.

Use the following procedure to select icons if the cursor is on a toolbar

- You can move the cursor by pressing the ← or → Key.
- If you press the **Enter** Key, the operation for the icon on which the cursor is present will be executed.

Enlarging and Shrinking the Program Window

The Program WIndow can be enlarged, shrunk, or adjusted to the window width to make it easier to view programs that have been created or that are being created.

Press the **Alt** + ← Keys to reduce the size of the section displayed in the Program Window. Press the **Alt** + → Keys to increase the size.

Undoing or Redo an Operation

You can undo an operation or redo an operation. These are convenient, e.g., when something is deleted accidentally. You can press the **Ctrl** + **z** Keys to undo and the **Ctrl** + **y** Keys to redo up to 100 operations.

15-4 Creating Program Projects

This section describes how to create and save program projects and set management data to program projects.

15-4-1 Creating Program Projects

When the Logic Editor is started from the Network Configurator, it retains the information that was set in the Network Configurator. Therefore the Controller model and other information will already be set in the Logic Editor project.

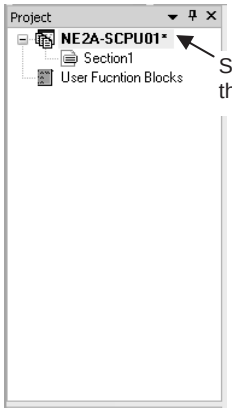
Changing the Project Name

The project name can be changed.

Procedure

1,2,3...

1. Select the project in the Project Window.
2. Select ***Rename*** from the Edit Menu, or press the shortcut key and select ***Rename*** from the menu.
   You will be able to change the project name in the Project Window.



3. Change the project name and press the **Enter** Key.

Note Up to 48 alphanumeric characters (48 bytes) can be entered for the project name. The characters that can be input are the same as those that can be input for variables. Refer to *Variable Specifications* on page 80. The project name is transferred to the Controller when the configuration is downloaded.

Saving Projects

To save projects that have been created or that are in the creation stage, close the Logic Editor and return to the Network Configurator.
Refer to *9-5 Saving and Reading Network Configuration Files* for details saving Network Configurator projects.

15-4-2 Setting Information in Projects

You can set information in the projects that you have created. The project information can be printed out.

Procedure

1,2,3...

1. Select ***Property*** from the Project Menu.
   You can also select the project from the Project Window, press the shortcut key and then select ***Property*** from the menus.
   The *Property* Dialog Box will be displayed.



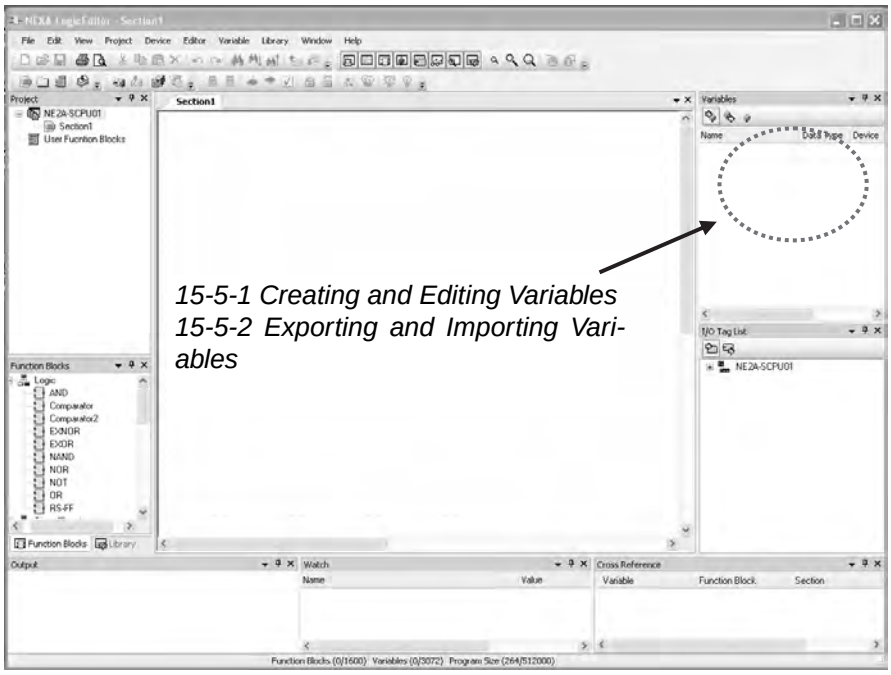
The date and time when the project was first opened or created will be displayed for the creation date, and the date and time when the project was last saved will be displayed for the last updated date.

2. Input the author, company name, and comment and then click the **OK** Button.

Note Up to 256 characters (256 bytes max.) can be used for the author, company name, and comment.

15-5 Creating Variables

A NE2A-series Safety Network Controller uses variables instead of I/O comments when creating programs.
By using variables, you can make programs without considering memory addresses, I/O allocations, or connection settings. This improves the reusability of program logic because I/O addresses are not used directly.



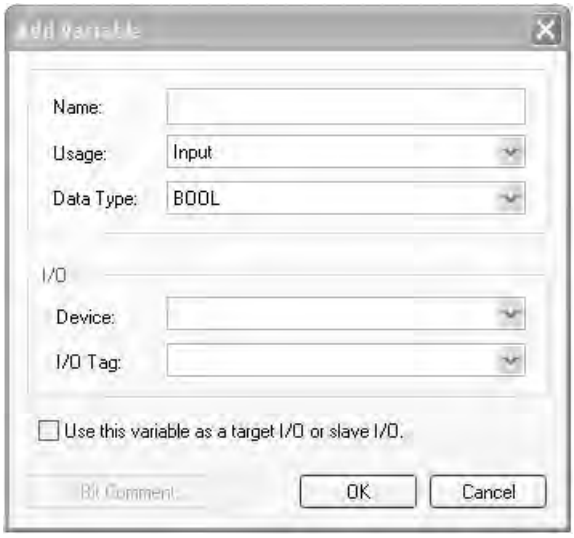
15-5-1 Creating and Editing Variables

If the I/O configuration is set beforehand, variables can be automatically created from the I/O tag list (see details in following section) or they can be automatically created by inserting them into sections in the Program Window from the I/O tag list. (Refer to *15-6-1 Arranging Input Variables* for information on inserting variables into sections.)

Creating New Variables

Procedure

1,2,3... 1. Select ***Add*** from the Variable Menu.
The Add Variable Dialog Box will be displayed.



2. Specify the variable parameter values and click the **OK** Button.
   The parameters are described in the following table.

Item	Description	
Name	Specifies the variable name. Up to 48 characters (48 bytes max.) can be used. Names are not case sensitive if ASCII alphabetic characters are used. The following characters cannot be used. :! # $ % & ' " ( ) = ~ ^ \ | ` @ { + ; * : } < , > ? / . [ ] Also the following cannot be used: • The first character cannot be a number. • Reserved characters cannot be used.	
Usage	Select from input, output, or internal.	
Data Type	Select from BOOL, BYTE, WORD, or DWORD.	
Device	Assigns the device's I/O tag to the variable.	Select the device of the I/O tag to assign to the variable from the list.
I/O Tag		Displays a list of the I/O tags of the selected device (only tags with the specified data type). Select the I/O tag to assign to the variable.

The maximum number of variables that can be created are given in the following table.

Data type	Bits	Maximum number of input and output variables	Maximum number of internal variables
BOOL	1	Total points: 2,048	Total points: 1,024
BYTE	8	All BOOL data: 2,048	All BOOL data: 1,024
WORD	16	All BYTE data: 256 *1	All BYTE data: 128 *2
DWORD	32	All WORD data: 128*1	All WORD data: 64*2
		All DWORD data: 64*1 *1: 2,048 points/number of bits	All DWORD data: 32*2 *2: 1,024 points/number of bits

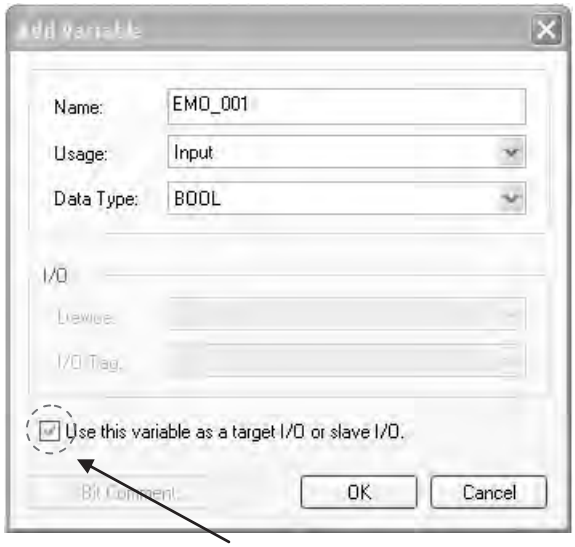
The following data types and attributes can be specified for each type of variable.

Item	Input variable	Output variable	Internal variable
Actual I/O allocation	Supported *1	Supported	Not supported
Bit comments	Supported	Supported	Supported

*1 Not supported for user-defined function blocks.

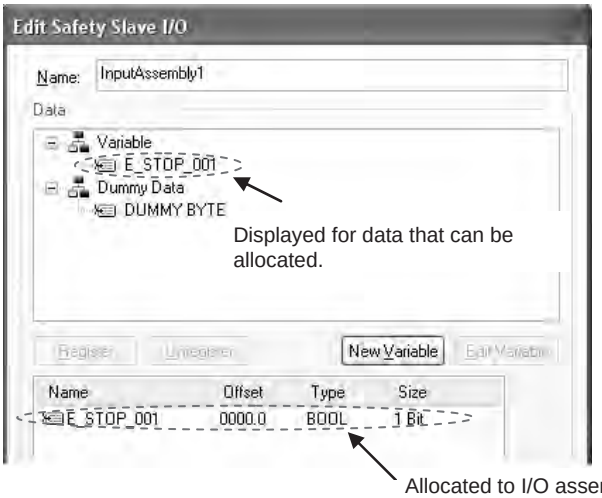
Target I/O and Slave I/O

When using a variable as a Target I/O or a Slave I/O, select the *Use this variable as a Target I/O or slave I/O* Option.



Select the check box.

The variables that have been created will be displayed in the data list that can be allocated to assembly data in the Edit Safety Target I/O, Edit Slave I/O (DeviceNet), and Edit Target I/O (EtherNet/IP) Dialog Boxes.
Refer to *11-5 Using the NE2A-series Controller as a Safety Slave*, *11-7 Using an NE2A-series Controller as a Standard Slave*, and *12-7 Using an NE2A-series Controller as a Standard Slave* for details on allocating variables.

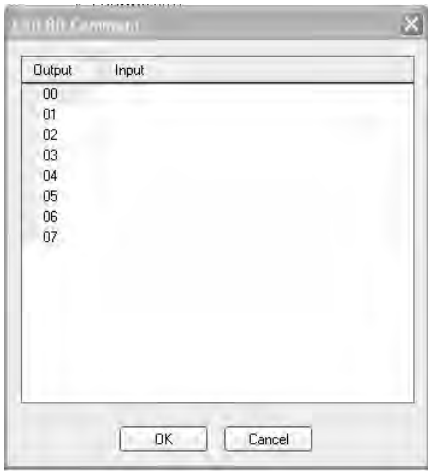


If the usage type is set to internal (i.e., internal variable), it cannot be used for Slave I/O. The setting to use it as Slave I/O or Target I/O will not be enabled.

Editing Bit Comments

A comment can be set for each bit if the data type is BYTE, WORD, or DWORD.

1,2,3... 1. Click the **Edit Bit Comment** Button.
The Edit Bit Comment Dialog Box will be displayed.



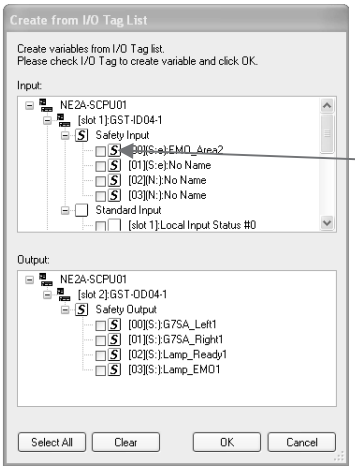
2. Enter a comment for each bit and press the **Enter** Key.
3. Clicking the **OK** Button will set the bit comment.

Note Up to 48 characters can be used for the bit comment (48 byte max.)
The characters that can be input are the same as those that can be input for variables. Refer to *Variable Specifications* on page 80.

Creating Variables from the I/O Tag List

If the remote I/O connection settings and local I/O settings are already set, variables can be automatically created from the actual I/O tag list. In this case, the variable name will be generated from the I/O comment name.

1,2,3... 1. Select ***Create from I/O Tag List*** from the Variable Menu.
The Create from I/O Tag List Dialog Box will be displayed.



Creates variables from selected I/O tags.

2. Select the I/O tags for the variables that you want to create and click the **OK** Button.
The I/O tags selected in the Variable Window will be registered as variables.

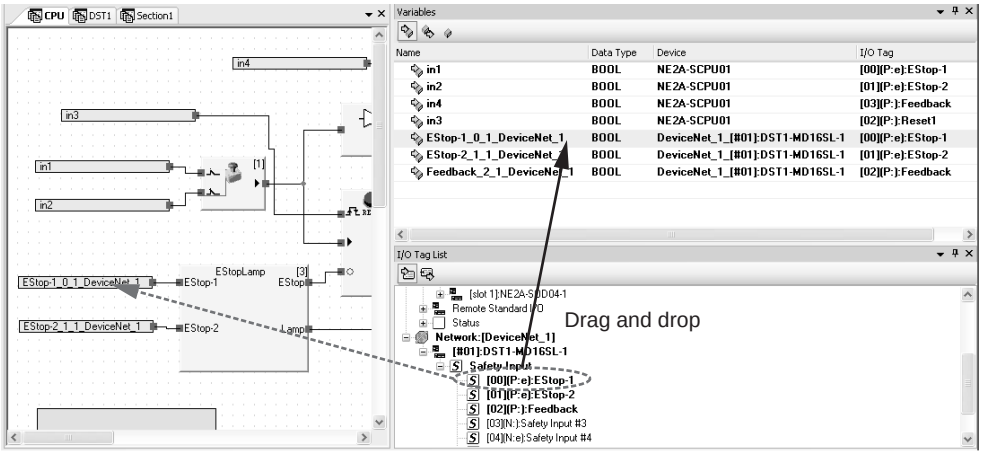
Note Click the **Select All** Button to select all I/O tags. Click the **Clear** Button to clear the selection of all I/O tags.

Dragging and Dropping from the I/O Tag List Window

You can automatically create a variable by dragging and dropping an I/O tag from the I/O Tag List Window to the Variable Window.

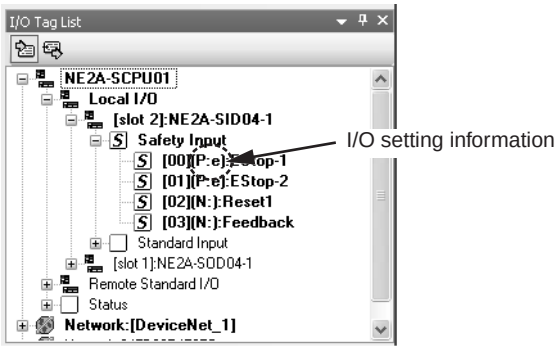
The variable type will be determined by the type of the I/O tag (input or output).

By dropping the selected I/O tag on top of an existing variable, you can perform the procedure for setting I/O tags.



Note When creating variables, if there are duplicated names or I/O tags, an error will occur. Also, when the number of registered variables exceeds the limit, adding more variables will cause an error.

The I/O settings are indicated with symbols on the I/O tag. The following list gives the meanings of the symbols.



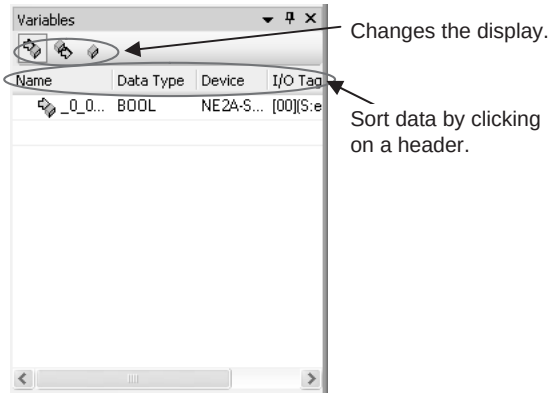
Symbol	Input Mode	Symbol	Channel Mode
N	Not used	None	Single Channel
P	Test pulse from test out	e	Dual Channel Equivalent
S	Used as safety input	c	Dual Channel Complementary
ST	Used as standard input	m	MAT

Symbol	Output mode	Symbol	Channel Mode
N	Not used	None	Single Channel
S	Safety	d	Dual Channel
P	Safety pulse test	---	---

Switching Displays

You can switch the display between input variables, output variables, and internal variables by clicking the buttons at the top of the Variable Window.

You can also sort the data by clicking on the column header, by Name, Data Type, Device, or I/O Tag. You can arrange the data in ascending or descending order by clicking on the header.



Changing Types

The input variable, output variable, and internal variable types can be changed.

Procedure

1,2,3...

1. Select the variable for which you want to change the type from the Variable Window.
2. Select ***Change Variable Type*** from the Variable Menu and select the type, or press the shortcut key and select ***Change Variable Type*** and the type from the menu.

The name and data type will be retained after changing the type, but the I/O tag allocation will be cancelled.

Copying, Pasting, and Cutting

Selected variables can be copied or cut.

If the same variable name already exists when pasting, the variable will be registered as *COPY (serial number)_name*. If a variable with the same I/O tag already exists when pasting, the variable will be registered as a non-allocated variable.

15-5-2 Exporting and Importing Variables

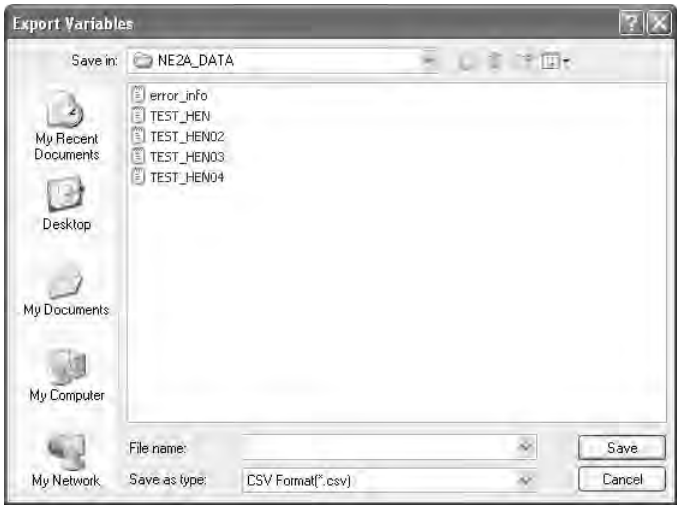
The variable data that you have created can be exported, and the exported file can be imported into another project. You can also export a list of I/O tags using ***Export Tags***. This is convenient to edit the exported variable file to change I/O assignments.

Exporting Variables

Procedure

1,2,3...

1. Select ***Export*** – ***Export Variables*** from the Variables Menu.
   The Export Variables Dialog Box will be displayed.

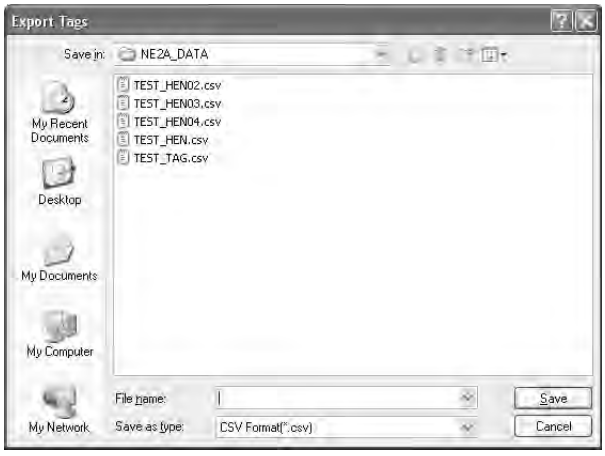


2. Specify the name and folder for the file to be exported, and click the **Save** Button.

Exporting Tags

Procedure

1,2,3... 1. Select ***Export*** – ***Export Tags*** from the Variables Menu. The Export Tags Dialog Box will be displayed.

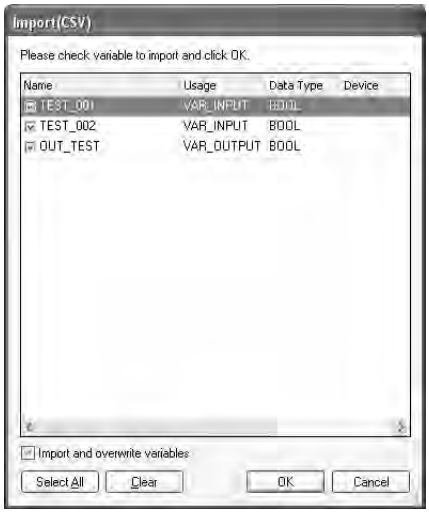


2. Specify the file name and folder to which to export the data and click the **Save** Button.

Importing Variables

Procedure

1,2,3... 1. Select ***Import*** from the Variable Menu.
The Import Dialog Box will be displayed.
2. Select the file to be imported.



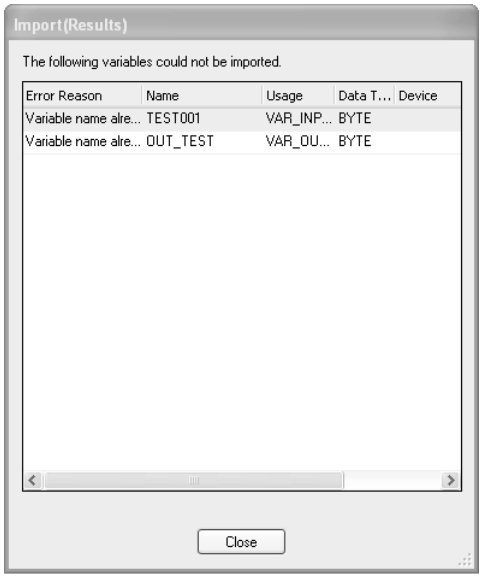
- If you click the **Select All** Button, all variables will be selected.
- If you click the **Clear** Button, the selection of all variables will be cleared.
- If you clear the selection of the *Import and overwrite variables* Check Box, variables will not be overwritten if variables with the same names are imported.

3. Select the variables to be imported, and then click the **OK** Button.
   The selected variables will be displayed in the Variable Window.

If the I/O tags specified in the variable data file do not exist, the file will be imported without any I/O allocations.

Import Errors

A list that shows the results of importing will be displayed. Detailed results of importing will be displayed in the Output Window.



15-5-3 Finding and Replacing Variables

Finding a Variable

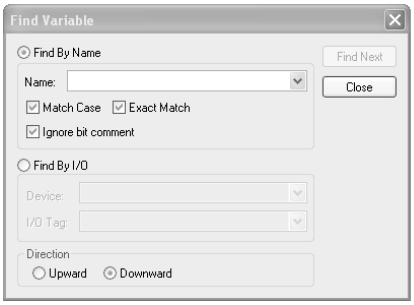
You can find a variable either by its name or by its I/O tag.

Procedure

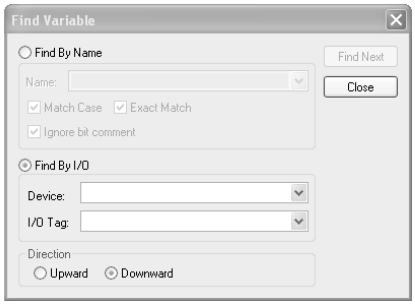
1,2,3...

1. Select the Variable Window.
2. Select ***Find*** from the Edit Menu.
   The Find Variable Dialog Box will be displayed.

Finding by name



Finding by I/O tag



3. Select whether you want to find the variable by name or by I/O. Specify either the name or the I/O tag of the variable, and then click the **Find Next** Button.

   The items in the dialog box are described in the following table.

Item	Description
Find By Name	Enables the user to find a variable by its name.
Name	Input the variable name to search for.
Match Case	Sets whether the search is case sensitive. Not selected: Do not match case. Selected: Match case.
Exact Match	Sets whether to find only exact matches. Not selected: Do not find only exact matches. Selected: Find only exact matches.
Ignore bit comment	Sets whether to search for bit comments. Not selected: Search for bit comments. Selected: Do not search for bit comments.
Find by I/O	Enables the user to find a variable by its I/O tag.
Device	Select the device to searched for.
I/O Tag	Select the I/O tag to searched for.
Direction	Sets the direction in which to search for variables. Upward: Search upward. Downward: Search downward.

4. To continue searching for more variables, click the **Find Next** Button.
5. To end your search, click the **Close** Button.

Replacing a Variable

You can replace a variable name.

Procedure

1,2,3...

1. Select the Variable Window.
2. Select ***Replace*** from the Edit Menu.
   The Replace Variable Dialog Box will be displayed.



3. Specify the variable name to be replaced, and then click the **Find Next** Button.
   The items displayed in the Replace Variable Dialog Box are described in the following table.

Item	Description
Name	Input the variable name to search for.
Replace	Input the variable name to be replaced.
Match Case	Sets whether the search is case sensitive. Not selected: Do not match case. Selected: Match case.
Exact Match	Sets whether to find only exact matches. Not selected: Do not find only exact matches. Selected: Find only exact matches.
Ignore bit comment	Sets whether to find and replace bit comments. Not selected: Find and replace bit comments. Selected: Do not find and replace bit comments.
Direction	Sets the direction in which to find the variables. Upward: Search upward. Downward: Search downward.

4. If you find a variable and want to replace it, click the **Replace** Button.
   If you do not want to replace the variable name, click the **Find Next** Button.
   If you want to replace all matching variables, click the **Replace All** Button. (All variables will be replaced without allowing you to check them.)

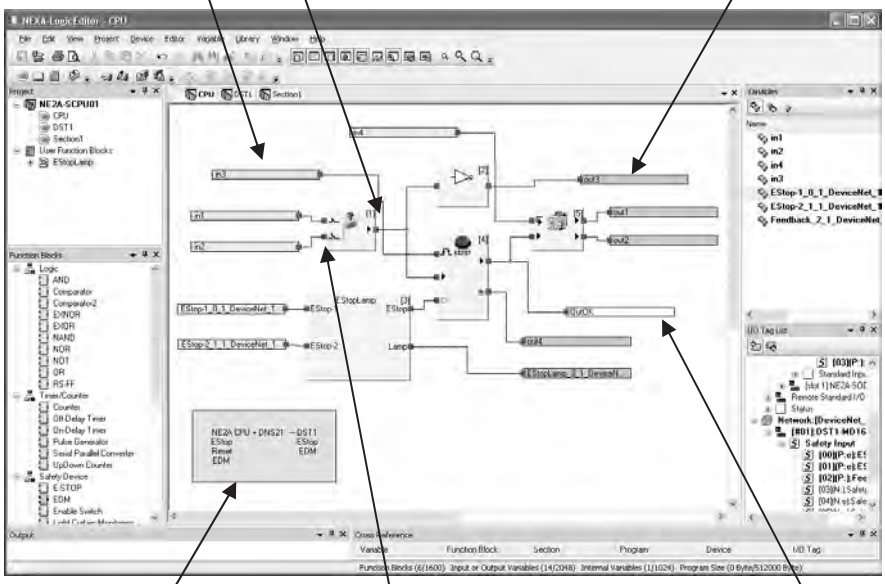
15-6 Creating Programs

Programs are created by arranging variables and function blocks. Refer to the *Safety Network Controller Command Reference Manual* (Cat. No. Z920) for details on function blocks.

15-6-1 Arranging Input Variables

15-6-2 Arranging Function Blocks
15-6-3 Function Block Settings

15-6-4 Arranging Output Variables



15-6-7 Arranging Text Boxes

15-6-6 Connecting Function Block Input/Output Signals

15-6-5 Arranging Internal Variables

15-6-1 Arranging Input Variables

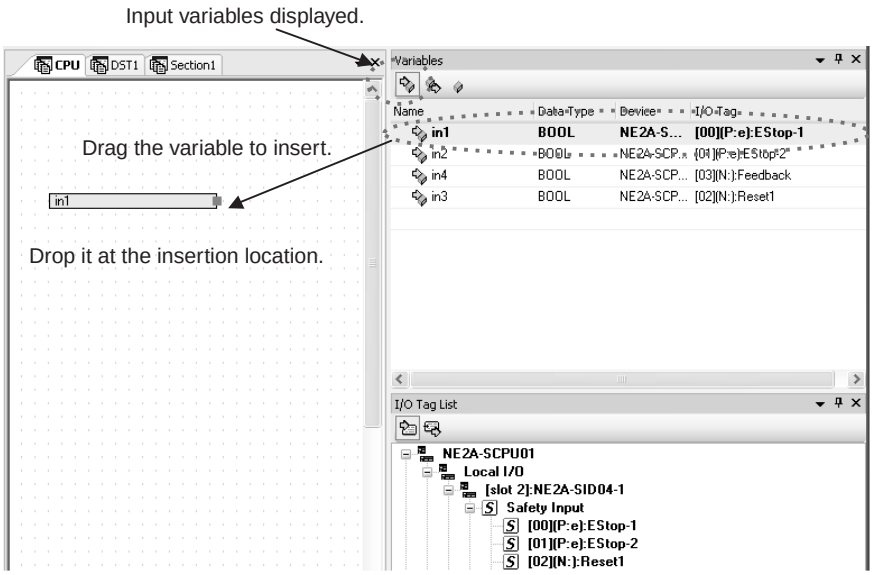
Variables can be inserted by dragging and dropping them or by using the I/O tag.

Inserting Variables by Dragging and Dropping

Procedure

1,2,3...

1. Display the input variables in the Variable Window.
2. Drag the variable that you want to insert from the variable list in the Variable Window.
3. Drop the variable in the desired position in the Program Window.



Note When a variable is used in a program, the variable name will change to bold in the Variable Window. If an I/O tag is assigned to a variable, the I/O tag name in the I/O Tag List Window will change to bold.

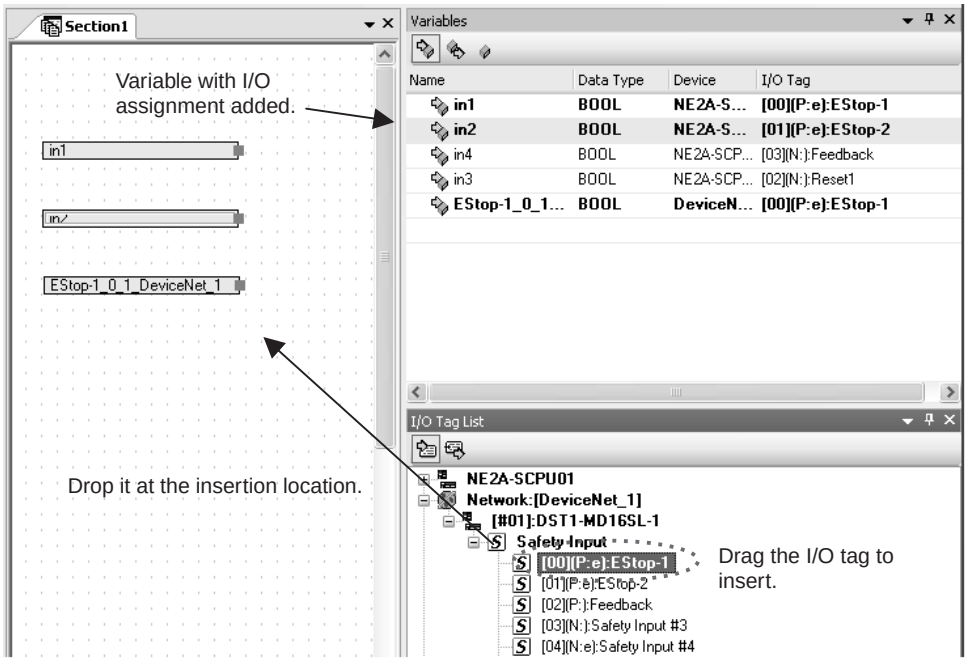
Inserting Variables from I/O Tags

Variables can be directly pasted in sections of the Program Window from the I/O tag list in the I/O Tag List Window.

Procedure

1,2,3...

1. Drag the I/O tag that you want to insert from the I/O Tag List Window.
2. Drop the I/O tag in the desired position in the Program Window. The variable allocated to the I/O will be added to the Variable Window.



Note When a variable is deleted from the variable list in the Variable Window, the arranged variable will also be deleted. The variable will not be deleted even if the I/O Unit settings of the I/O tag assigned to the variable are changed.

15-6-2 Arranging Function Blocks

You can insert function blocks by dragging and dropping them using the mouse.

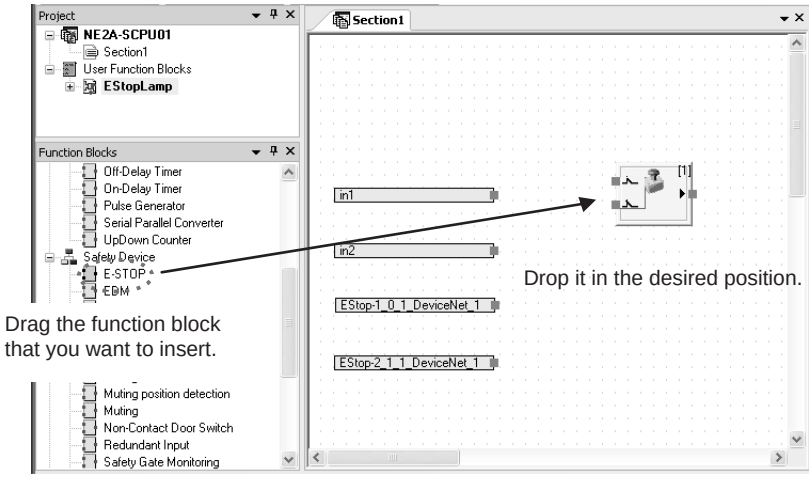
To arrange a function block, insert an existing function block or user-defined function block.

Inserting Function Blocks by Dragging and Dropping

Procedures

1,2,3... 1. Drag the function block that you want to insert from the Function Blocks Window.

2. Drop the function block in the desired position in the Program Window.



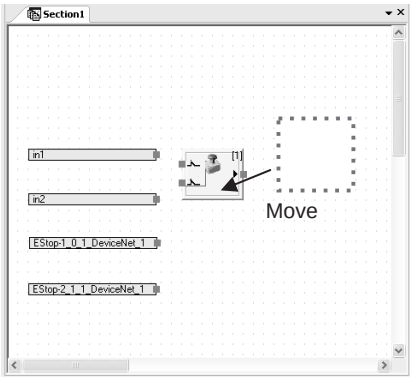
Moving Function Blocks

Use one of the following procedures to move a function block.

- Drag and drop the function block with the mouse.
- Move the function block by using the keys.

1,2,3... 1. Select the function block to be moved with the **Tab** Key.

2. Move the function block with the ↑, ↓, ←, or → Key.



Placement Errors

An error message will be displayed if you attempt to place a function block at a location where it cannot be inserted.



If the function block cannot be inserted, insert it at another location temporarily, and then move it with the mouse to the desired location. The mouse pointer will change to an prohibited mark (⃠) at locations where you cannot insert a function block.

If an error message is displayed when you cannot insert a user-defined function block or a variable, insert it at another location temporarily, and then move it with the mouse to the desired location.

15-6-3 Function Block Settings

The number of input and output terminals can be changed from the default value for some function blocks. Change the input and output terminals according to the function block logic.

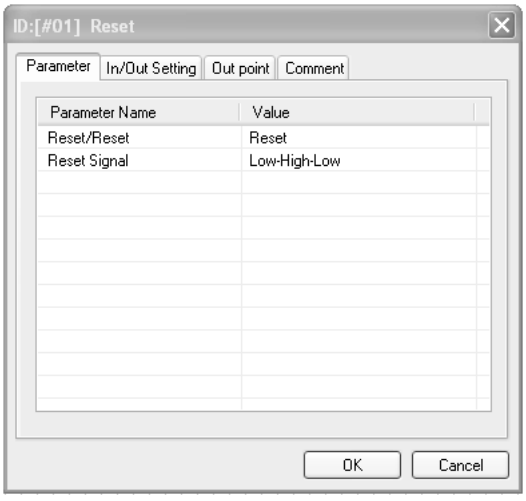
Refer to the *Safety Network Controller Command Reference Manual* (Cat. No. Z920) for details on the function block settings.

This section shows how to change the settings for a Reset function block.

Procedure

1,2,3...

1. Select the Reset function block.
2. Select ***Settings*** from the Editor Menu, or press the shortcut key and select ***Settings*** from the menu. The Function Block Settings Dialog Box will be displayed. (The Function Block Settings Dialog Box varies with the selected function block.)

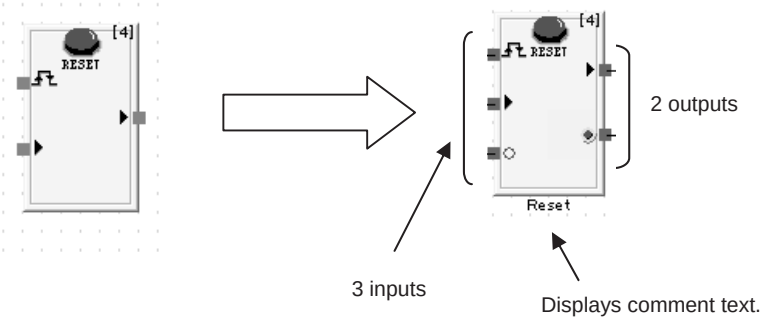


3. Set the parameters and click the **OK** Button

For details on parameters, refer to the *NE2A Series Safety Network Controller Command Reference Manual* (Cat. No. Z920).

For example, the Reset function block settings will be changed as shown in the following diagram. The changes are listed in the following table.

Tab page	Parameter	Default value	Modified value
In/Out Setting	**Inputs**	2	3
Out point	**Static Release**	No check	No check
	Reset Required Indication	No check	Check
Comment	**Text**	Blank	“Reset”



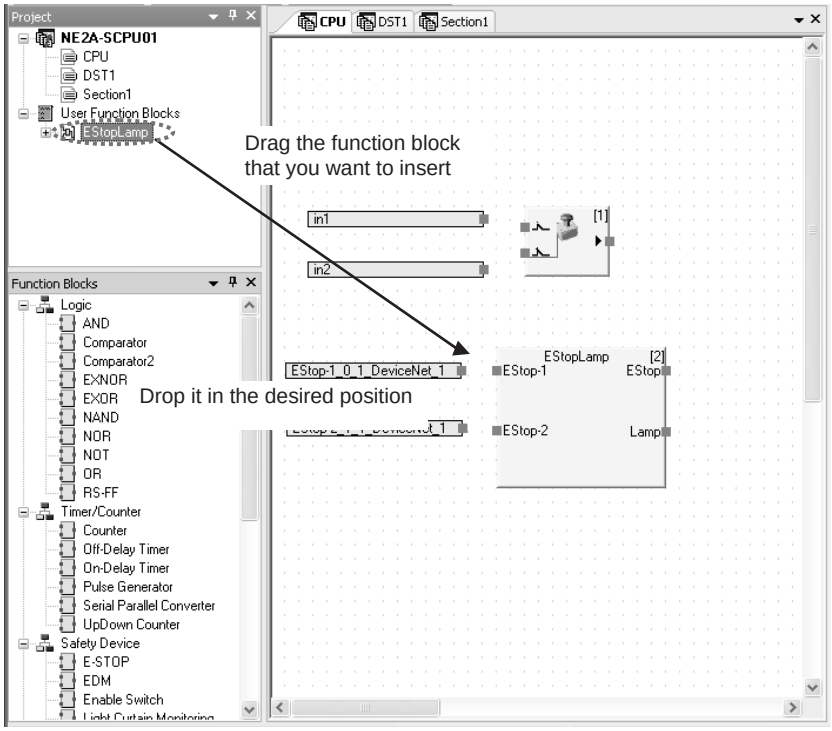
Arranging User-defined Function Blocks

User-defined function blocks can be inserted by using the same steps as inserting existing function blocks.

Procedure

1,2,3...

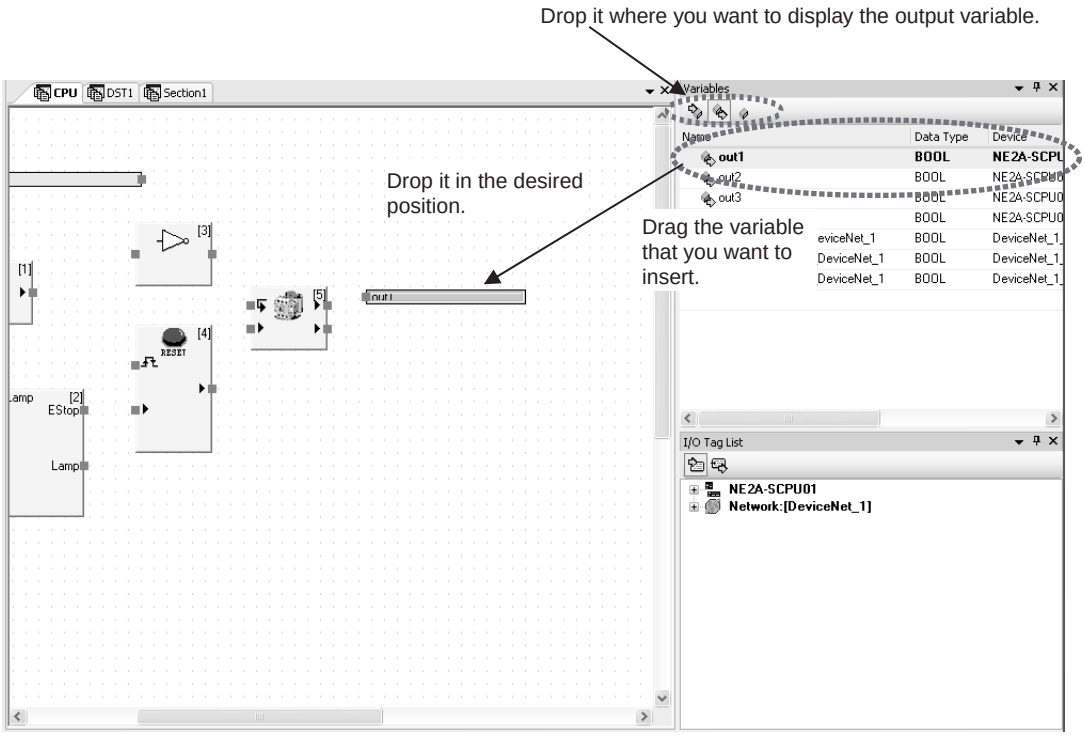
1. Drag the user-defined function block that you want to insert from the Project Window.
2. Drop the function block in the desired position in the Program Window.



If you delete a user-defined function block from the list of user-defined function blocks in the Project Window, the user-defined function block in the Program Window will be deleted.

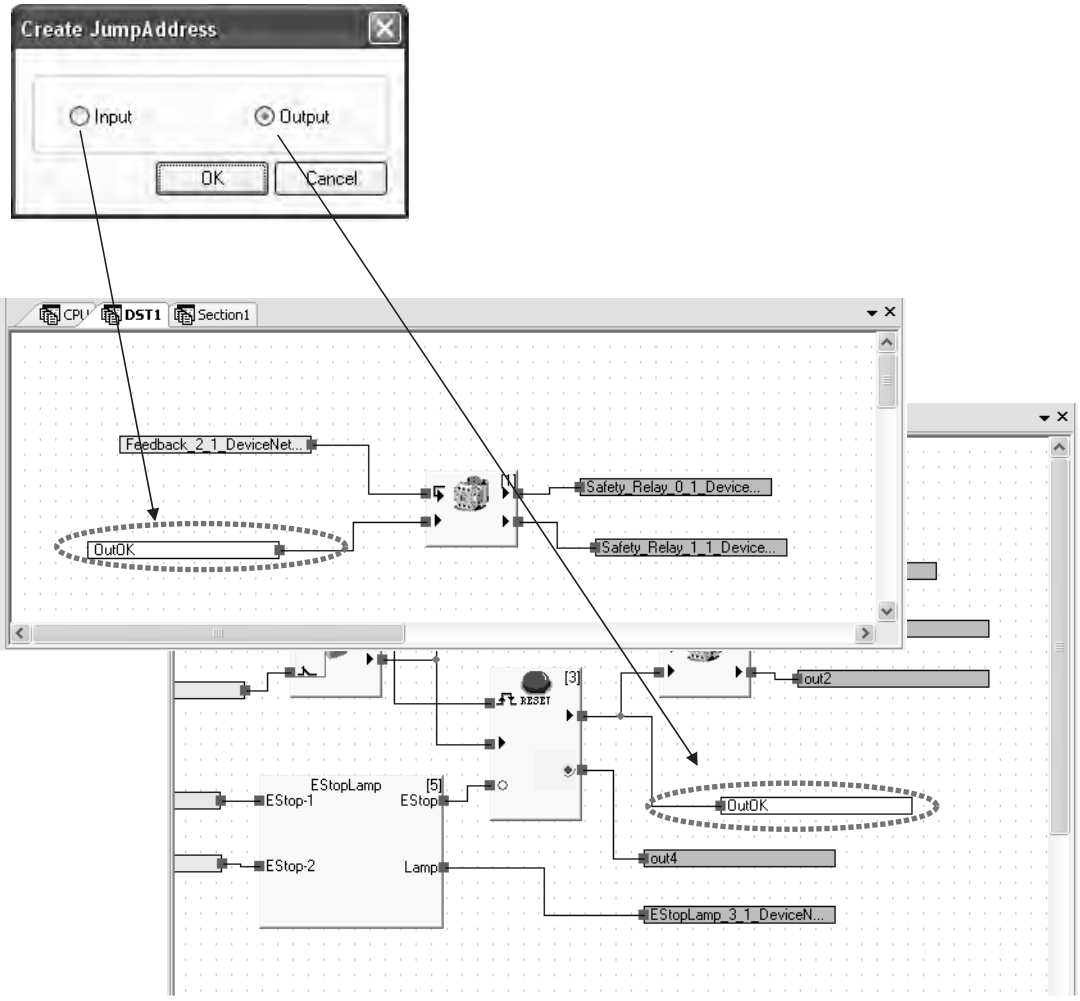
15-6-4 Arranging Output Variables

Like input variables, output variables can be inserted by dragging and dropping them or by using the menus. For information on the procedure, refer to *15-6-1 Arranging Input Variables*.



15-6-5 Arranging Internal Variables

Like input variables, you can insert internal variables by dragging and dropping them or inserting them using the menu. The following dialog box will be displayed if an internal variable is inserted. Set whether to use the internal variable as function block input data or output data.



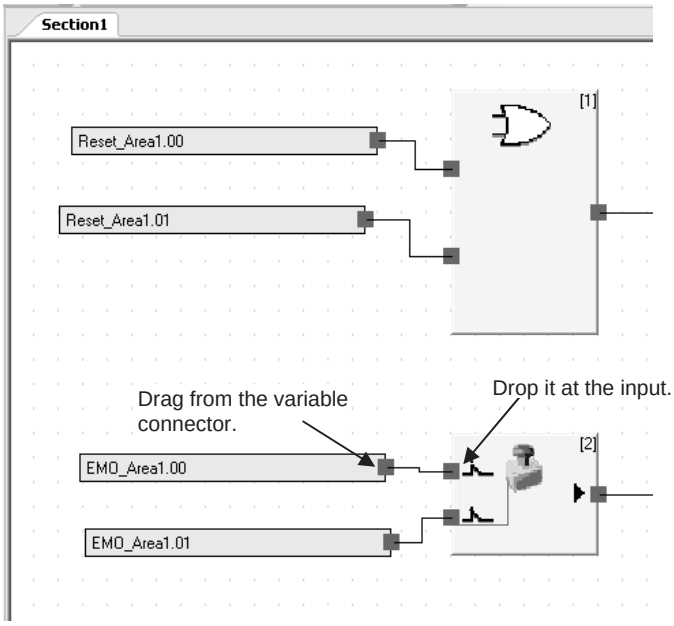
Internal variables must be used both as inputs and outputs. An error will occur in building the program if an internal variable is used only as an input or only as an output.

15-6-6 Connecting Function Block Input/Output Signals

You can connect the input/output signals between variables and function blocks as well as between different function blocks by dragging and dropping.

Dragging and Dropping

1,2,3... 1. Click a connector (■) and drag the line to another connector.



If the connection is invalid, an error message will be displayed.



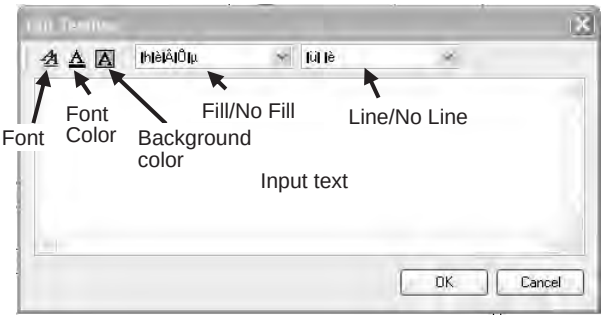
15-6-7 Arranging Text Boxes

Text boxes can be arranged in a program. You can paste comments or precautions related to the circuit in these text boxes.

Inserting Text Boxes

Procedure

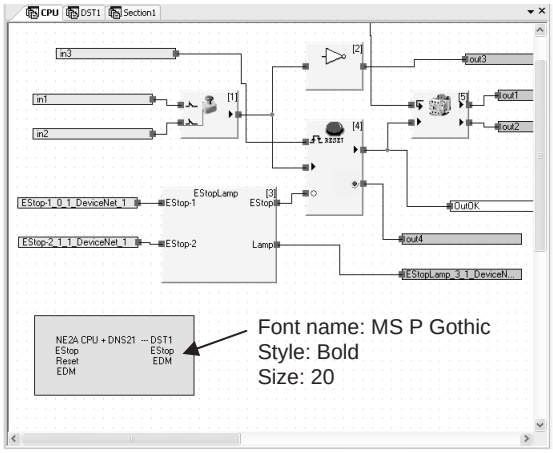
1,2,3... 1. You can select the desired location in the Program Window, press the shortcut key, and then select ***Insert - Text Box*** from the menu.
The Edit Text Box Dialog Box will be displayed.



2. Input the characters to be displayed in the text box, and set the font and font color, and the background color. The items displayed in the Edit Text Box Dialog Box are described in the following table.

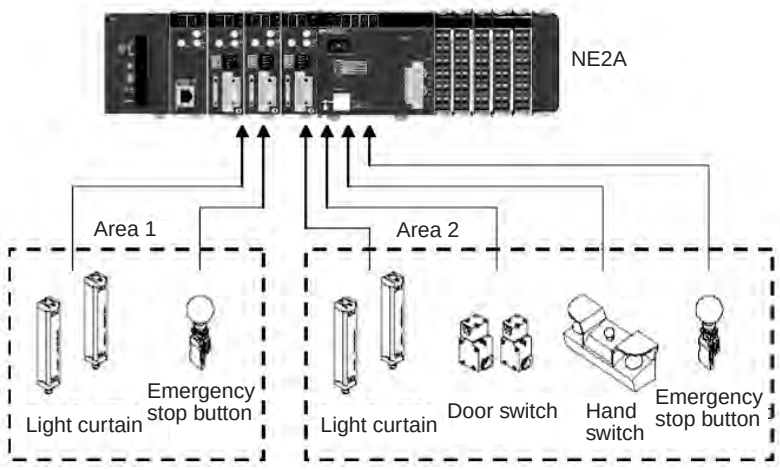
Item	Contents
Font	Sets the following items for the characters: • Font name, style, size, character format, and character set
Font color	Sets the font color.
Background color	Sets the background color.
Fill / No Fill	Sets whether the background of the text box is filled.
Line / No Line	Sets whether the border of the text box is displayed.
Input text	Sets the characters to be displayed in the text box.

3. The text box will be inserted when you click the **OK** Button.



15-7 Creating Sections

With a NE2A-series Controller, it is possible to connect many local I/O and remote I/O. With large-scale programs, the program structure may become complex and difficult to read, and arranging function blocks and variables may be restricted. If the same program structure is used in many locations, it is possible to create and copy program sections as sections.



For the system configuration shown above, separating the system into area 1 and area 2 makes it easier to understand. Also, separating light curtains and emergency stop buttons that are connected to both areas makes it easier to determine which light curtain or emergency stop button has an error if an error occurs.

15-7-1 Creating Sections

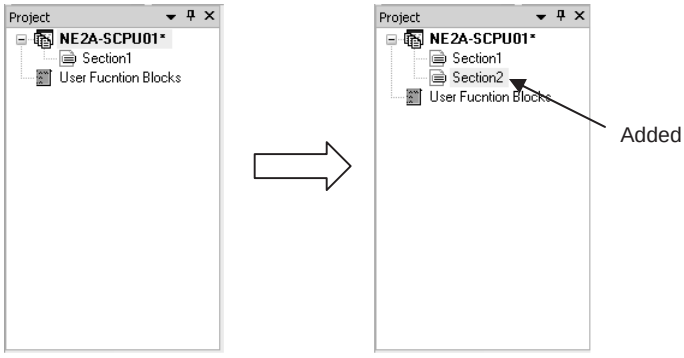
Projects can consists of more than one section. The sections can be used to separate the programming for individual functions and processes. This feature of the NE2A Safety Network Controller is useful when constructing large-scale systems because you can reduce maintenance by dividing the program into sections.

Adding Sections

When a new project is created, there is only one section. The following procedure can be use to add other sections.

Procedure

1,2,3... 1. Select ***Create New - Section*** from the Project Menu, or select a project or section from the Project Window, press the shortcut key, and select ***New Section*** from the menu.
A new section will be added to the project in the Project Window.



Note Up to 256 sections can be created.

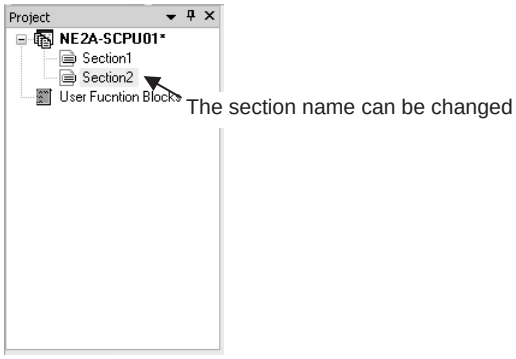
Note
(1) The NE2A-series Controller executes the program in order from the first (i.e., top) section registered in the Project Window.
(2) A list of the sections and folders are displayed in the Project Window. If you click a section, it will be displayed in the Program Window.

Changing Section Names

You can change the names of sections.

Procedure

1,2,3...
1. Select the section whose name is to be changed from the Project Window.
2. Select ***Rename*** from the Edit Menu.
   You can also press the shortcut key and select ***Rename*** from the menu.
   You will be able to change the section name in the Project Window.



3. Change the section name, and then press the **Enter** Key.

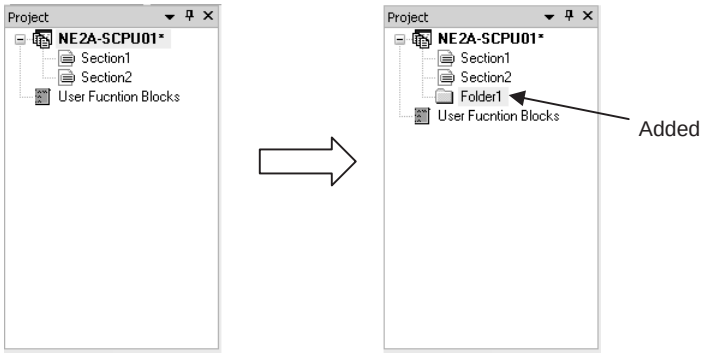
Note Up to 48 characters (48 bytes max.) can be used for the section name.
The characters that can be input are the same as those that can be input for variables. Refer to *Variable Specifications* on page 80.

Creating Folders

Folders can be created and used to group multiple sections.

Procedure

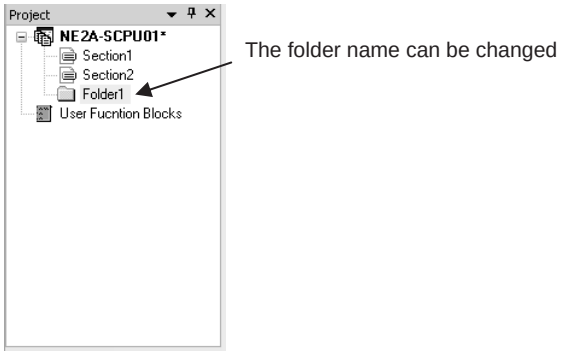
1,2,3...
1. Select ***Create New - Folder*** from the Project Menu, or select a project or section from the Project Window, press the shortcut key, and select ***New Folder*** from the menu.
   A folder will be added to the project in the Project Window.



Note
- Only one level of folders can be created. You cannot create folders within folders.
- Up to 256 folders can be created.

Changing the Folder Name

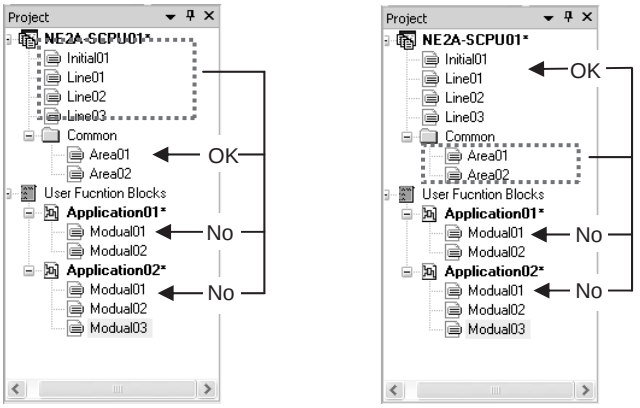
The procedure to change the name of a folder is the same as the procedure to change the name of a section. Select the folder and then perform the procedure.



Note Up to 48 characters (48 bytes max.) can be used for the folder name.
The characters that can be input are the same as those that can be input for variables. Refer to *Variable Specifications* on page 80.

Copying, Pasting, Cutting, and Deleting

You can copy or delete a section or folder.



A section cannot be pasted to a lower level of a user-defined function block

A section can be pasted only within the same project.

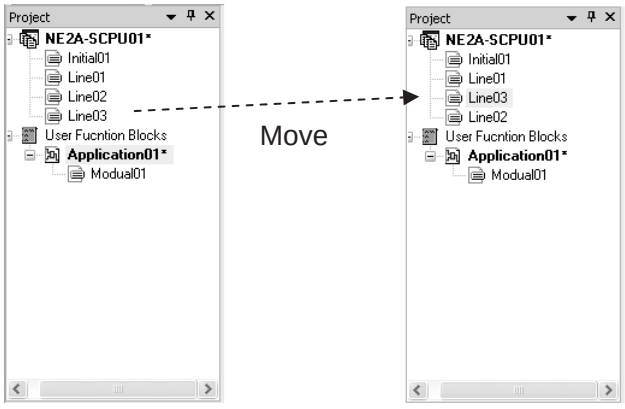
If the same section name already exists when pasting, the section will be registered as *COPY (serial number)_name*. If the length of the section name exceeds the limit, you cannot paste the section.

You cannot copy, cut, or paste folders.

Moving Sections Up and Down

Operations are executed first for the section listed at the top, and then for the sections listed below. You can change the order in which to operate the sections by moving the sections either by dragging and dropping them using the mouse, or by selecting ***Move Upward*** or ***Move Downward*** from the Edit Menu.

For example, you can move the section Line03 below the section Initial in the following three ways:



- Drag the section Line03 with the mouse, and drop it above the section Line01.
- Select the section Line03, and press the ↑ Key twice while keeping the **Ctrl** Key pressed.
- Select the section Line03, and click ***Move Upward*** twice in the Edit Menu.

15-8 Checking Programs

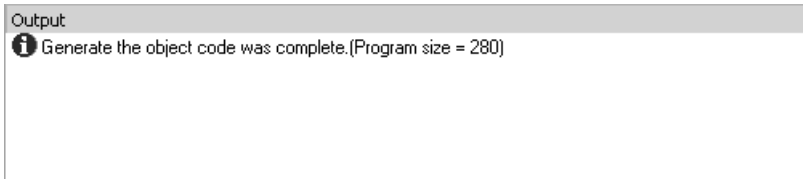
Programs must be checked to be sure they are written correctly and to be sure that variables are used correctly.

⚠ WARNING

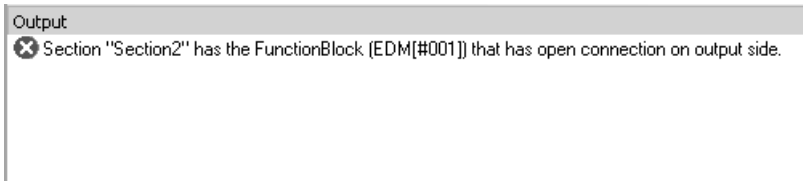
Serious injury may possibly occur due to loss of required safety functions. Be sure to sufficiently check all parameters related to safety functions.

15-8-1 Checking Programs for Syntax Errors

Check the programs you create for syntax errors. Start the check by selecting *Build* from the Project Menu. If there are no errors, the following message will be displayed in the Output Window.



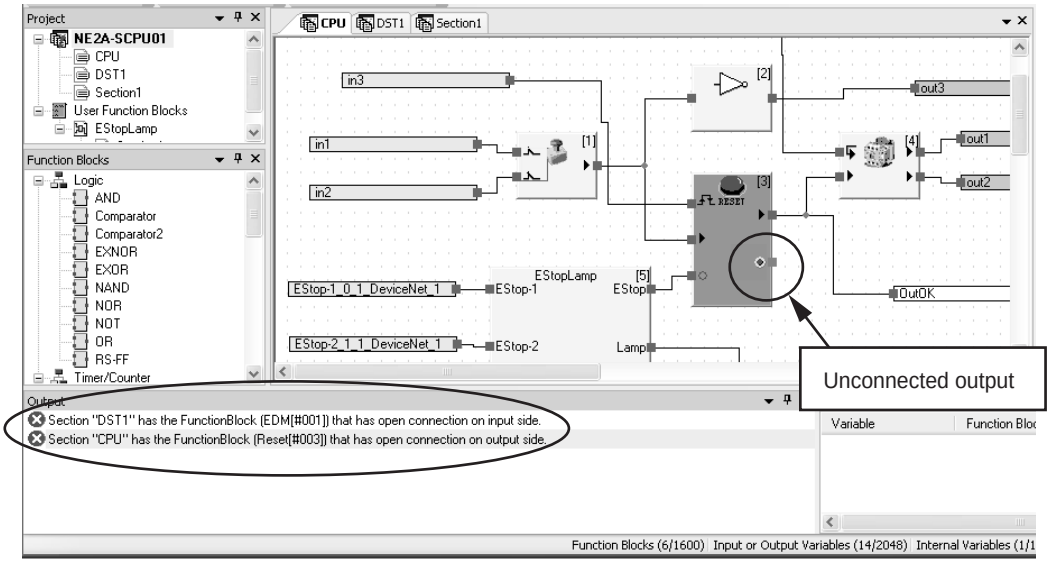
If an error is detected, the following error message will be displayed in the Output Window.



]

Searching for Unconnected Function Blocks

It is not possible to download a program if there are function blocks with unconnected inputs or outputs in it. (Refer to the following figure.) All I/O must be connected.



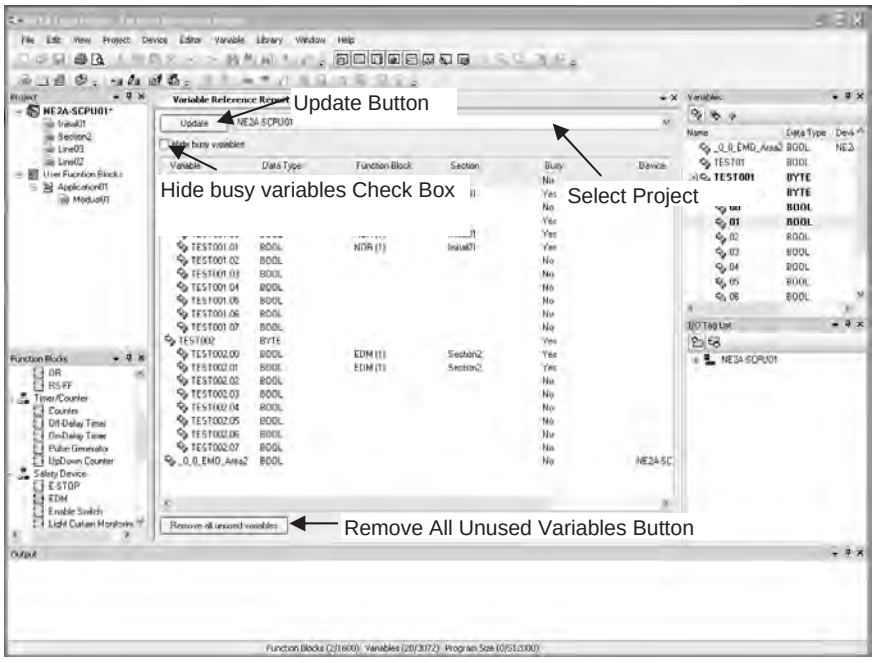
When a program is built (by selecting *Build* from the Project Menu), function blocks that have unconnected I/O will be displayed in the Output Window. Double-click the message to display the function block with unconnected I/O.

15-8-2 Displaying the Variable Reference Report

The sections in which the variables are being used and the function blocks to which the variables are connected can be displayed in a list.

Procedure

1,2,3... 1. Select ***Variable Reference Report List*** from the Variable Menu.
The Variable Reference Report Window will be displayed in the Program Window.



2. Select a project in the Select Project Area.
The usage status of all of the variables in the project will be displayed.

Displayed item	Contents
Variable	Displays all variables of the selected project.
Data Type	Displays the data type of the variables.
Function Block	Displays the connected function block name.
Section	Displays the section name in use.
Busy	Displays whether a variable is being used (Yes: Busy, No: Unused).
Device	Displays devices with I/O allocations.
I/O Tag	Displays I/O tags with I/O allocations.

Multiple items will be displayed if the same variable is used in multiple locations.
If you double-click a variable in use, the locations where it is in use will be displayed, and the variable will flash.

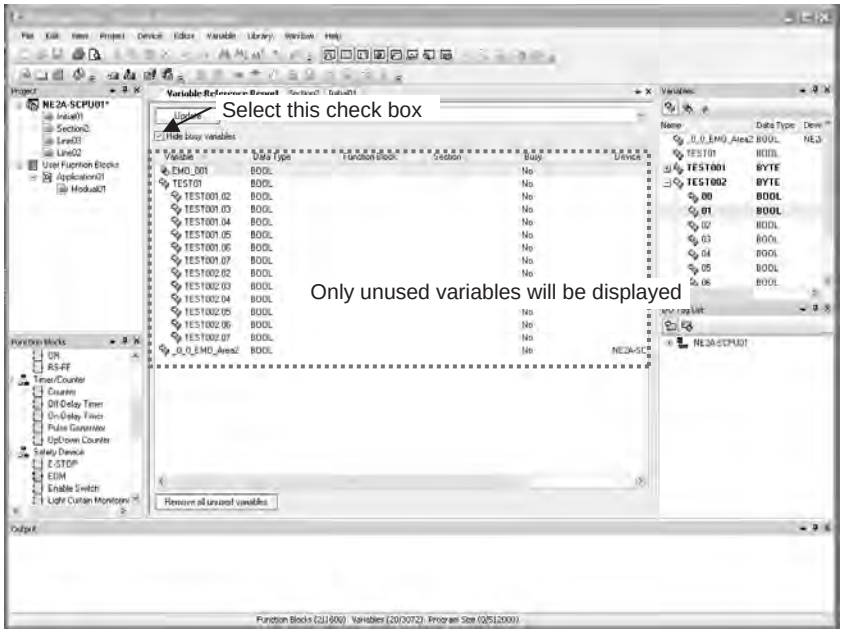
Updating the Information

If you click the **Update** Button, the information of the Variable Reference Report Window will be updated to the most recent information.

Once the Variable Reference Report Window is displayed, it will turn gray when there is a change in a variable. Click the **Update** Button to update the display.

Displaying Unused Variables

If you select the *Hide busy variables* Check Box, only the unused variables will be listed in the window.



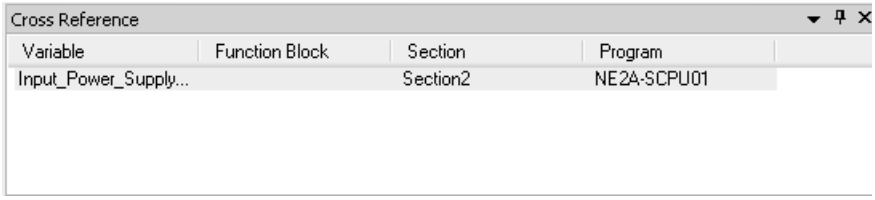
Deleting Unused Variables

If you click the **Remove all unused variables** Button, the variables for which No is displayed in the Busy Area of the window will be deleted.

15-8-3 Searching

Cross References

The Cross Reference Window displays a list of where in which section a variable is being used. For each variable, the program name, section name, and function block I/O where it is connected will be displayed.
Double-click the displayed variable to cause the variables in used in the Program Window to begin flashing.

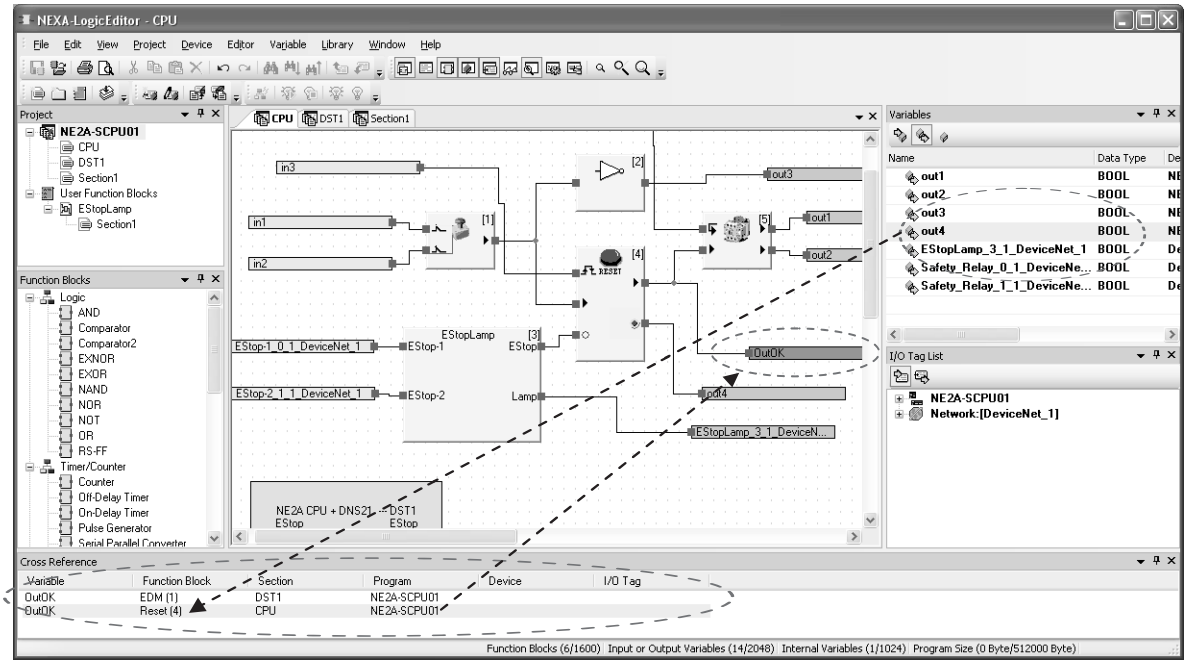


Searching for Variables in the Program

You can search for the section in which a variable is used.

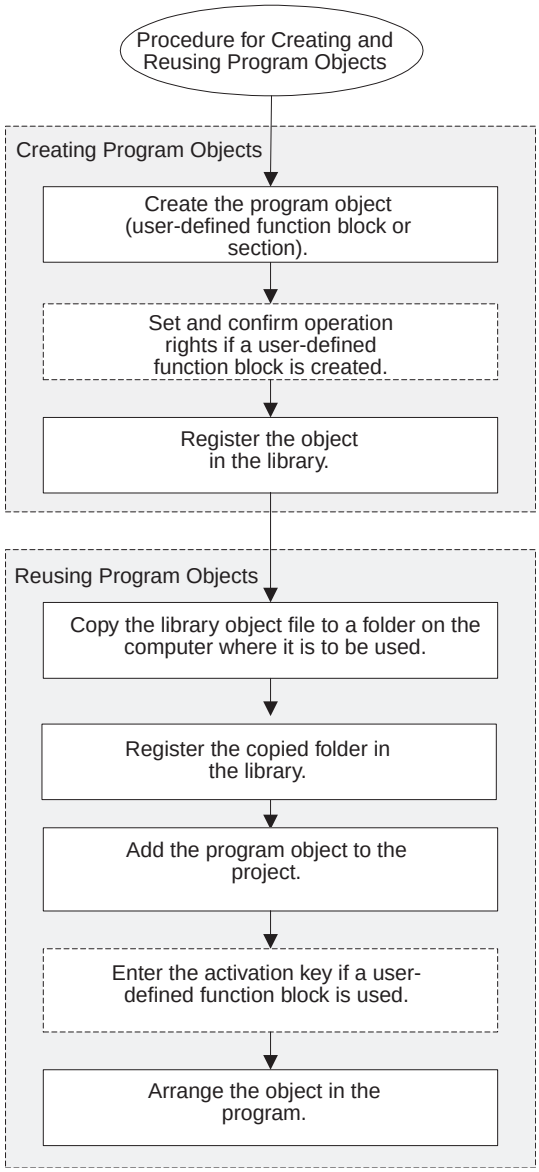
1,2,3... 1. Select the variable that you want to search for from the Variable Window. The variable information will be displayed in the Cross Reference Window.

2. Double-click the variable in the Cross Reference Window.
   The section where the variable is used will be displayed and the variable in the Project Window will begin flashing.



15-9 Creating and Reusing Program Objects

Sections and user-defined function blocks can be saved as objects and reused.
It is also possible to import programs created using an NE1A-series Controller and reuse them on an NE2A-series Controller.



IMPORTANT To perform the following procedures, start the Network Configurator as the system administrator. (Refer to *9-4-1 Starting and Exiting the Network Configurator*.)

- Saving, deleting, and importing user-defined function blocks.
- Registering folders in the library or deleting folders from the library.
- Registering user-defined function blocks and sections in the library.

On Window 2000 or XP, these operations are not possible unless you are logged on with administrator rights.
On Windows Vista or 7, if the above operations are preformed when the Network Configurator is started without administrator rights, Windows Vista/7 user account management will redirect you to the local folder of the user that started the Network Configurator. The results of these operations will therefore not be applied for other user accounts.

Operation Rights for User-defined Function Blocks

Operation rights for user-defined function blocks are controlled by passwords and activation keys. The following rights apply to operations to user-defined function blocks.

		Editing	Browsing and monitoring	Using user-defined function blocks in programming
Password	**Editing**	Yes	Yes	Yes
	Browsing	No	Yes	Yes
Activation key		No	No	Yes

For details on the activation keys, refer to *7-1-4 User-defined Function Block Passwords*.

To set the operation rights, select the user-defined function block and select the Project Menu. The following settings can be made for operation rights of user-defined function blocks.

Menu command	Description
Authentication	Authenticates the password for a user-defined function block with a password setting to enable accessing and editing the function block.
Change Password	Changes the password required to access and edit a user-defined function block.
Display Activation Key	Enables checking the activation key required to reuse user-defined function blocks from a library.

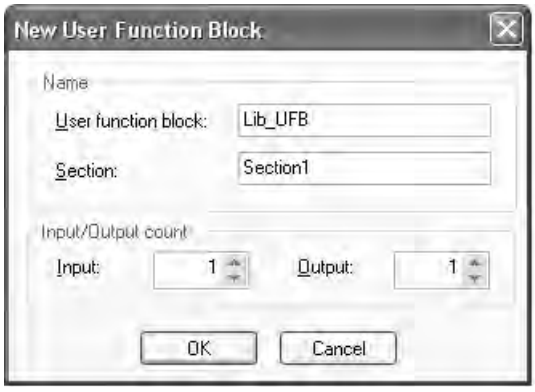
Note There are no operation right settings for sections.

15-9-1 Creating User-defined Function Blocks

You can create new function blocks by combining the function blocks that are provided with the Network Configurator.

Procedure

1,2,3... 1. Select ***New - User Function Block*** from the Project Menu.
Or, select **User Function Block** in the Project Window, and then right-click *New User Function Block*.
The New User Function Block Dialog Box will be displayed.



2. Set the user function block name, section name, the number of inputs, and the number of outputs. The displayed numbers of inputs and outputs will change according to the inputs and outputs that are added to or deleted from the user-defined function block.
3. Click the **OK** Button.
   The Set Password Dialog Box will be displayed.
4. Set the password for editing and the password for browsing, and then click the **OK** Button.
   The user-defined function block will be added to the *User Function Blocks* Folder in the Project Window.

Note
(1) Each password can be set using up to 16 alphanumeric characters. The following characters cannot be used in names of user-defined function blocks: \ / : ; * ? < > | & ‘ “

(2) If the OK Button is clicked without setting a password, no password will be set, i.e., no password will be required for editing or browsing.

5. Create the program.
   Select the section for the user-defined function block and create the program using the same procedure as in *15-6 Creating Programs*. If required, add variables and create sections and folders.
   The Program WIndow of the user-defined function block will turn gray.
6. Save the user-defined function block.
   Select ***User Function Block - Save*** from the File Menu.
   If a user-defined function block used in the program is edited, the user-defined function block used in the program will also be updated when it is saved.

Note
(1) I/O tags cannot be used in user-defined function blocks.

(2) It is not possible to use user-defined function blocks in a user-defined function block.

IMPORTANT When you change the parameters of the NE2A-series Controller, always be sure that all of the user-defined function blocks that are used in the program are installed first.
When parameters are changed for a NE2A-series Controller that includes user-defined function blocks in the program, information that is included in the user-defined functions blocks is used not only in the program, but it is also used in other ways, such as in calculating the cycle time.

IMPORTANT If a user-defined function block that is used in more than one NE2A program is changed, you must rebuild all the programs that use the user-defined function block to reflect the changes.

Example: If program A and program B use the same user-defined function block and the user-defined function block is changed in program B after program A has been built, the changes in the user-defined function block will not be reflected in program A. To reflect the changes, you must rebuild program A.

You can restrict access to user-defined function blocks to prevent unintentional changes to them. Refer to *7-1-4 User-defined Function Block Passwords* for the setting procedure.

Importing User-defined Function Blocks

It is necessary to import a user-defined function block to use it in a program.

- Select ***User Function Block - Import*** from the File Menu.

15-9-2 Creating Program Objects

This section describes the procedure for managing user-defined function blocks and sections.

Note Sufficiently confirm safety before providing user-defined function blocks and sections as objects to other people for use in programming.

Specifying the Library Folder Where the Object File Is Stored

Specify the folder in which to store the object file as a library object. Select ***Window - Library*** from the Display Menu to display the Library WIndow. “Library” will be displayed as the default folder in the Library Window.

Note The default Library Folder is C:\Program Files\OMRON\Network Configurator v3\NExA Programmer\Library. C:\Program Files\OMRON\Network Configurator v3 is a folder installed by the Network Configurator.

Use this procedure to create a new folder.

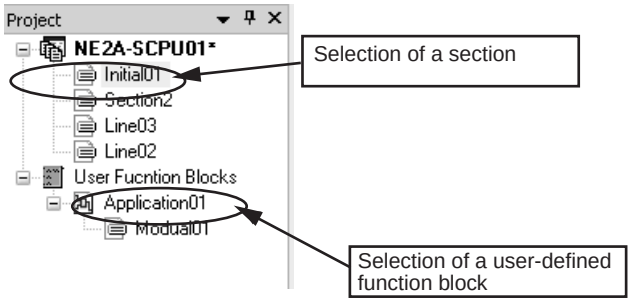
1,2,3...

1. Select ***Map Folder*** from the Library Menu.
   The Browse Folder Dialog Box will be displayed.
2. Specify the folder for storing the files and click the **OK** Button.
   The specified folder name will be displayed in the Library Window.

Adding Objects to the Library

1,2,3...

1. In the Project Window, select the user-defined function block or section that you want to save.



2. Select ***Add to Library*** from the Library Menu, or drag and drop the user-defined function block or section to the Library Window.
   The Register Library Item Dialog Box will be displayed.



3. Set the parameters and click the **OK** Button.
   The parameter settings are described in the following table.

Parameter	Description
Name	Sets the user-defined function block.
Description	Sets a description.
Author	Sets the author's name.
Company	Sets the company name of the author.
Version	Sets the version of the user-defined function block.
Register to	Sets where to register the user-defined function block.

4. The Activation Key Dialog Box will be displayed if a user-defined function block is used. Enter the activation key, and then click the **OK** Button.



The user-defined function block or section will be added to the library objects in the Library Window. The user-defined function block or section will also be created in the specified folder. Distribute this file as the program object.

Note

(1) The project file (*.nvf file) and user-defined function block file (*.udf file) are saved as separate files.

(2) The following apply if a section that uses I/O tags is created as a library object.

- I/O tags assigned to variables are removed from the variables.
- I/O tags are removed from variables generated from I/O tags only the variable names are left. If, however, an I/O tag is assigned to a variable of the same name that is already defined when the library object is read from the library into the project, that assignment will be used.

15-9-3 Reusing Programming

Copy the file created in the above section *15-9-2 Creating Program Objects* to a computer to reuse it. If you copy the file to a folder under C:\Program Files\OMRON\Network Configurator v3\NExA Programmer\Library, you need not perform the operation given below in *Preparing to Reuse a File*.

Preparing to Reuse a File

When preparing to reuse an object, register a folder to store the user-defined function block or section in the Library Window.

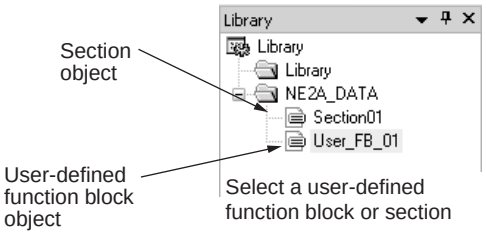
1,2,3...

1. Select ***Map Folder*** from the Library Menu.
   A dialog box will be displayed where you can browse the folders.
2. Specify the folder in which the file is saved, and click the **OK** Button.
   The folder name specified in the Library Window will be displayed.

Adding Function Blocks and Sections to a Project

1,2,3...

1. In the Library Window, select the user-defined function block or section you want to save.



2. Select ***Add to Project*** from the Library Menu.
   You can also drag the selected user-defined function block or section using the mouse, and then drop it in the Project Window.
   a. User-defined Function Block
      The Import Authentication Dialog Box will be displayed.



   a.1. Select the *Use Activation Key* Option or the *Use Password* Option.
      When a valid value has been set, the OK Button will be enabled.
   a.2. Click the **OK** Button.
      The Add to Project Dialog Box will be displayed.



   b.1. Section
      The Add to Project Dialog Box shown above will be displayed.
3. Specify the items to be set, and then click the **OK** Button.
   The items displayed in the Add to Project Dialog Box are described in the following table.

Item	Description
Name	Set the name for the selected object to be used in the program.
Settings	Adds a suffix to the variable name used in the object. If the variable name in the program being created and the variable name in the object are the same, they will be treated as the same variable. A prefix is added to enable differentiating the variable in the object. The setting is enabled if the object is a section.

   The user-defined function block or section will be added to the program.

15-9-4 Importing NE1A-series Programs

The NE2A-series Controller can import programs from an NE1A-series Controller. This enables efficient use of existing NE1A-series Controller programming assets.

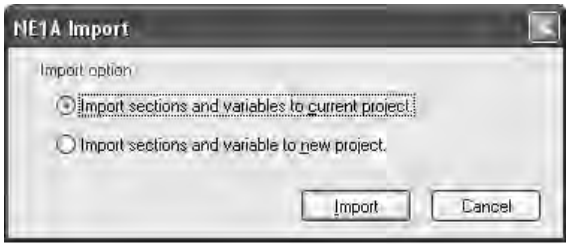
NE1A Logic File

Programs created using the NE1A-series Controller can be imported to the Logic Editor of an NE2A-series Controller. The programs to import from the NE1A-series Controller are exported from the Logic Editor of the NE1A-series Controller (created in a *.led file). Refer to the *DeviceNet Safety System Configuration Operation Manual* (Cat. No. Z905).

Procedure to Import to the NE2A-series Controller

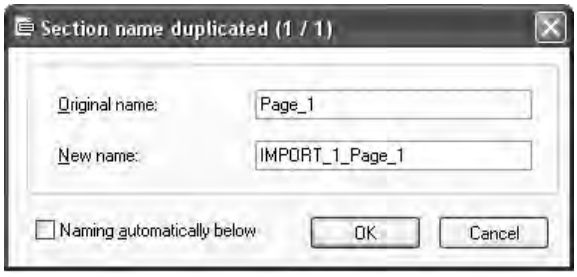
1,2,3... 1. Select ***Import - NE1A Logic File*** from the File Menu.

2. Select the NE1A-series Controller program file (*.led) to be imported in the NE1A Import Dialog Box.
The NE1A Import Dialog Box will be displayed.



3. Select the *Import Option* Option, and then click the **Import** Button.
The file will be added to the Project Window.

The following dialog box will be displayed to confirm name change if there is already a section or variable with the same name.



Note I/O tag names for NE1A-series programs will be converted to variables names that are not assigned to I/O when the I/O tag names are imported to the NE2A-series Controller.

Importing NE1A-series User-defined Function Blocks

User-defined function blocks that were created with an NE1A-series Controller can be used as user-defined function blocks for an NE2A-series Controller. The NE1A-series user-defined function block to import is exported using the Logic Editor of the NE1A-series Controller. (A *.fbd file is created.) Refer to the *DeviceNet Safety System Configuration Operation Manual* (Cat. No. Z905).

Procedure for Importing to an NE2A-series Controller

1,2,3... 1. Select ***Import - NE1A Function Block*** from the File Menu.

2. Select the NE1A-series user-defined function block file (*.fbd) to be imported in the Open File Dialog Box.

Note If a NE1A-series user-defined function block with a password is read into an NE2A-series Controller, the password setting will be removed.

15-10 Printing

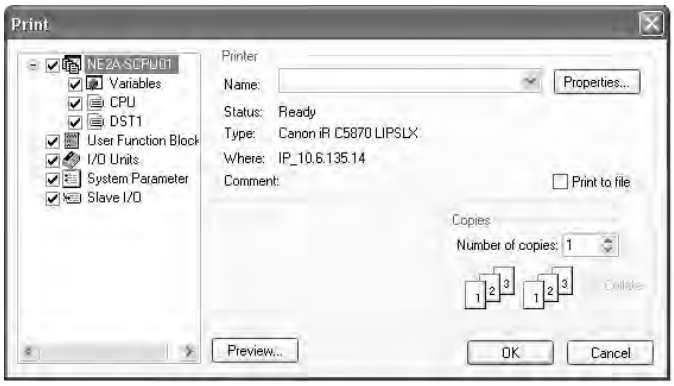
Programs can be printed. The printer settings can be made and a print preview can be viewed.

15-10-1 Printing

Use the following procedure to print the program.

Procedure

1,2,3... 1. Select ***Print*** from the File Menu.
The Print Dialog Box will be displayed.



What happens after clicking the **Property** Button varies with the type of printer, so no description is given here.

2. Select the information to be printed.
The print information is listed in the following table.

Print information		Description
NE2A-SCPU01	**Variable**	Sets whether to print information on variables.
	Section	Sets whether to print sections.
User-defined Function Block		Sets whether to print user-defined function blocks.
I/O Unit		Sets whether to print I/O Units.
System Settings		Sets whether to print the system settings.
Slave I/O		Sets whether to print Slave I/O.
Printer	**Printer**	Sets the printer.
	Status	Displays the status of the selected printer.
	Type	Displays the type of the selected printer.
	Location	Displays the location of the selected printer.
	Comment	Displays the comment for the selected printer.
	Output to file	Sets whether to output the information to a file.
No. of Copies	**No. of copies**	Sets the number of pages to print.
	Print in sections	Sets whether to collate the copies.

3. Click the **OK** Button to begin printing.
   - Click the **Cancel** Button to stop the printing process.
   - Click the **Preview** Button to display the Print Preview Window.
   - Refer to *15-10-2 Print Preview* for details on the Print Preview.

Printing

Printing is performed with the following page format.

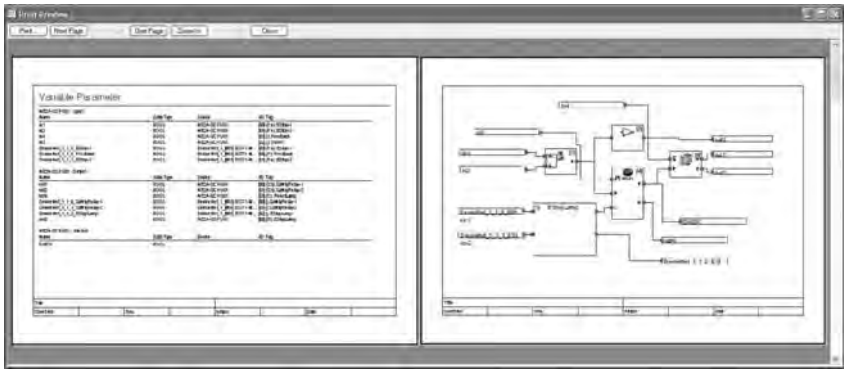
Page		Description
NE2A-SCPU01	Variable list	The variable names, data types, devices, I/O of the I/O tags, and internal variables will be printed, in that order.
	Program	The program will be printed.
User-defined Function Block	Variable list	The variable names, data types, devices, I/O of the I/O tags, and internal variables will be printed, in that order.
	Program	The program will be printed.
I/O Unit		The set values of the I/O Unit will be printed.
System Settings		The set values from the system settings will be printed.
Target I/O		The values of the Target I/O assembly data will be printed.

15-10-2 Print Preview

The print results can be checked on the computer.

Procedure

1,2,3... 1. Select ***Print Preview*** from the File Menu.
The Print Preview Dialog Box will be displayed.



The operation performed by each button is described in the following table.

Button	Description
Print	The Print Dialog Box will be displayed. Refer to *15-10-1 Printing*, for details on the Print Dialog Box.
Next Page	Switches to the next page. This button is disabled on the last page.
Prev Page	Switches to the previous page. This button is disabled on the first page.
One Page/Two Page	Switches between One Page/Two Page display in the preview. *The **Two Page** Button is enabled when one page is being viewed, and similarly, the **One Page** Button is enabled when two pages are being viewed.
Zoom In	Magnifies the view of the preview. The view can be magnified up to two levels.
Zoom Out	Returns the magnified view of the preview to normal. The view that was magnified up to two levels can be reduced up to two levels and returned to the standard view.
Close	Closes the Print Preview Window.

15-10-3 Page Setup

The paper size for printing, paper source, and print orientation can be specified.

Procedure

1,2,3... 1. Select ***Page Setup*** from the File Menu.
The Page Setup Dialog Box will be displayed.



The printer properties are not described in this section because they are different for each printer.

2. Specify the orientation, and click the **OK** Button.
The items displayed in the Printer Settings Dialog Box are described in the following table:

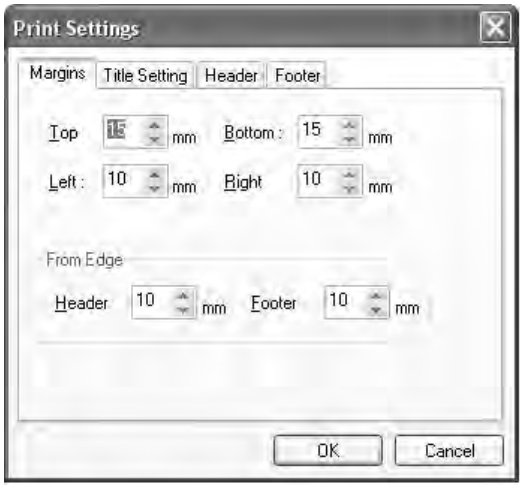
Item	Description
Size	Sets the size of the paper.
Source	Sets the paper source.
Orientation	Sets the orientation of the paper.

15-10-4 Printer Settings

The paper margins, title setting, header, and footer can be specified.

Procedure

1,2,3... 1. Select ***Printer Settings*** from the File Menu.
The Print Settings Dialog Box will be displayed.



2. Set the distance from the edge of the paper, and then click the **OK** Button. The items displayed in the Page Setup Dialog Box are described in the following table.

Tab name	Item	Contents
Margins	**Top**	Sets the size of the upper margin of the paper.
	Bottom	Sets the size of the lower margin of the paper.
	Right	Sets the size of the right margin of the paper.
	Left	Sets the size of the left margin of the paper.
	Header	Sets the print position of the header.
	Footer	Sets the print position of the footer.
Title Setting	**Lines**	Sets the number of title lines.
	Position	Sets the display position of the titles.
	Line	Sets the title line.
	Edit Line - Line Style	Sets the style of the title line.
	Edit Line - Title	Sets the title for each column.
	Edit Line - Contents	Sets the contents for each column title.
	Font – Font Name	Sets the font name to use for the title.
	Font - Style	Sets the style of the title.
	Font - Size	Sets the font size to use for the title.
	Font - Character Set	Sets the language to use for the title.
Header	**Left**	Sets the items to be printed in the left header.
	Center	Sets the items to be printed in the center header.
	Right	Sets the items to be printed in the right header.
Footer	**Left**	Sets the items to be printed in the left footer.
	Center	Sets the items to be printed in the center footer.
	Right	Sets the items to be printed in the right footer.

SECTION 16
Mounting, Wiring, and Hardware Settings

This section provides information necessary to install a NE2A-series Safety Network Controller, including hardware settings.

16-1 Installation Procedure 408
16-1-1 Installation and Wiring Precautions 408
16-1-2 Installation in Control Panel 408
16-1-3 Mounting I/O Units. 411
16-1-4 Mounting Communications Units. 412
16-1-5 Mounting the DIN Track 413
16-1-6 Removing an I/O Unit 413
16-1-7 Removing a Communications Unit 415
16-2 Wiring 416
16-2-1 General Precautions and Reference for Performing Wiring. 416
16-2-2 Applicable Wire Sizes, Crimp Terminals, and Tightening Torque. . 417
16-2-3 DeviceNet Wiring. 419
16-2-4 Ethernet Wiring. 419
16-3 Hardware Settings. 422

16-1 Installation Procedure

16-1-1 Installation and Wiring Precautions

Take the following points into consideration before installing the NE2A-series Controller to increase the reliability of the system and to ensure that the functionality of the system is not impaired.

Installation

Do not drop the NE2A-series Controller or subject it to excessive vibration or shock. The NE2A-series Controller may be damaged and may not function properly if it is mishandled.

Installation and Storage Environment

Do not use or store the NE2A-series Controller in any of the following locations:

- Locations subject to direct sunlight
- Locations subject to temperatures or humidity outside the range specified in the specifications
- Locations subject to condensation as the result of severe changes in temperature
- Locations subject to corrosive or flammable gases
- Locations subject to dust (especially iron dust) or salts
- Locations subject to water, oil, or chemicals
- Locations subject to shock or vibration that exceeds the specifications

Take appropriate and sufficient measures when installing systems in the following locations.

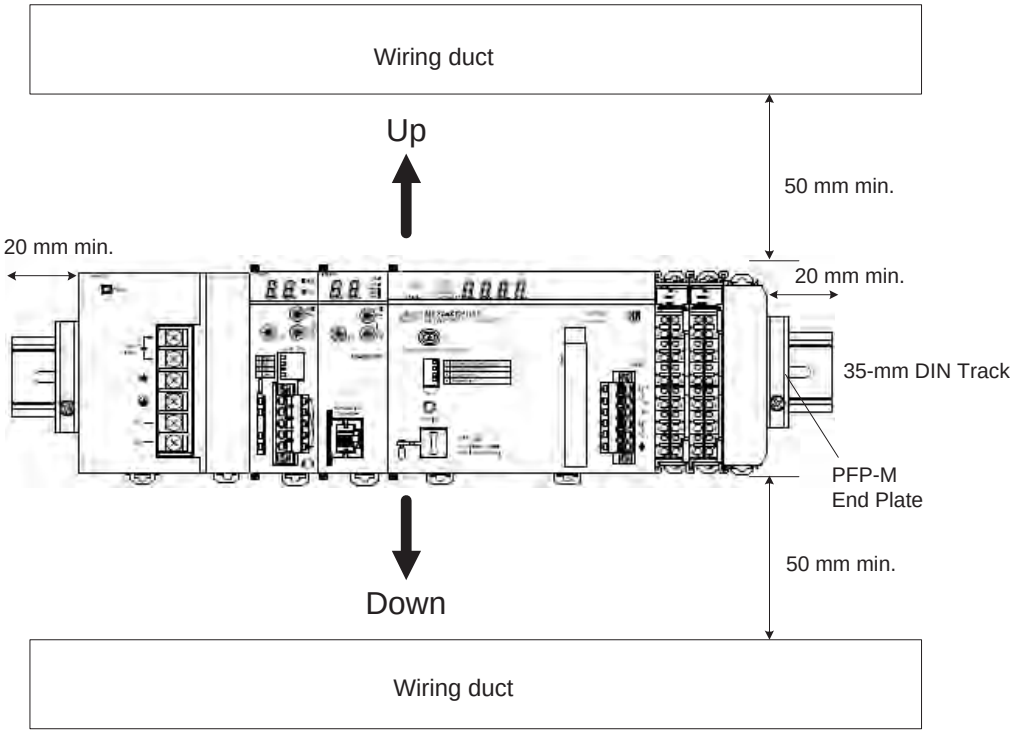
- Locations subject to static electricity or other forms of noise
- Locations subject to strong electromagnetic fields
- Locations subject to possible exposure to radioactivity
- Locations close to power lines

16-1-2 Installation in Control Panel

- The NE2A-series Controller must be installed in a metal cabinet that is connected to ground.
- Use the NE2A-series Controller within an enclosure with IP54 protection or higher (IEC/EN 60529).
- Use a DIN Track (TH35-7.5/TH35-15 according to IEC 60715) to install the NE2A-series Controller on the control panel. Mount the NE2A-series Controller to the DIN Track using PFP-M End Plates (not included with the NE2A-series Controller) to prevent it from falling off the DIN Track because of vibration.
- Do not use a cable that is longer than 3 m for the power supply.

Unit Installation Position

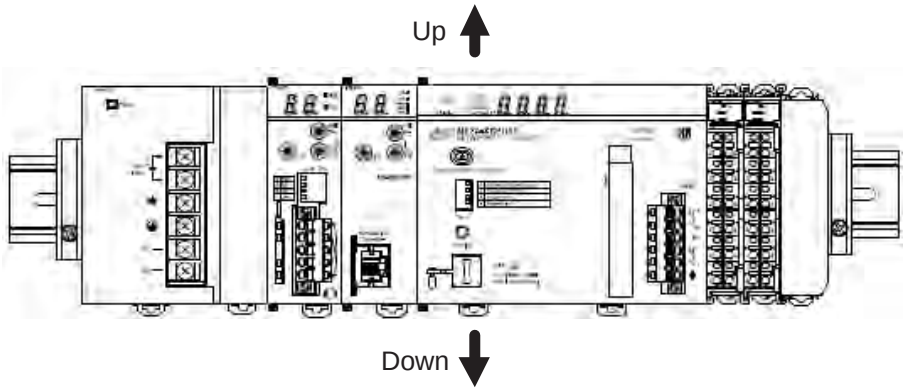
- Allow sufficient space, as shown in the following figure, between the top, bottom, and front of the NE2A-series Controller and the control panel or parts in the control panel to facilitate ventilation, wiring, and easy Unit replacement.



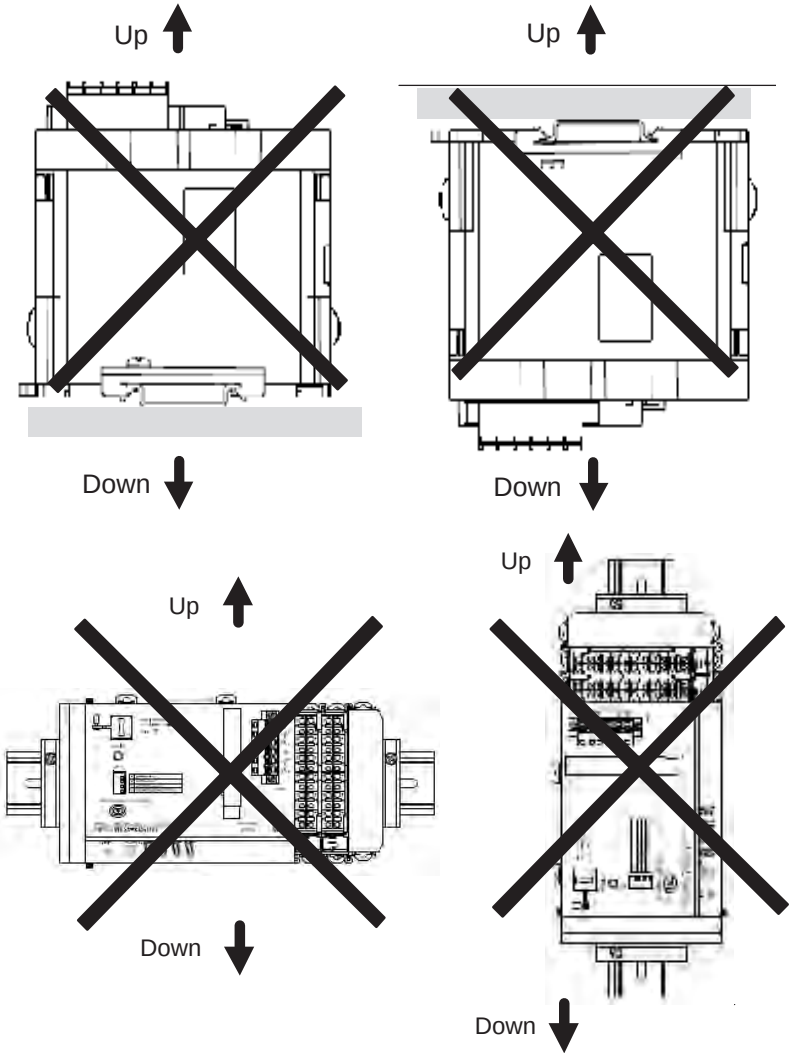
Note NE2A-series Controllers can be mounted only with a DIN Track. Mounting directly with screws is not possible.

Unit Installation Direction

To ensure heat dissipation of the NE2A-series Controller, use only the installation direction shown in the following figure.



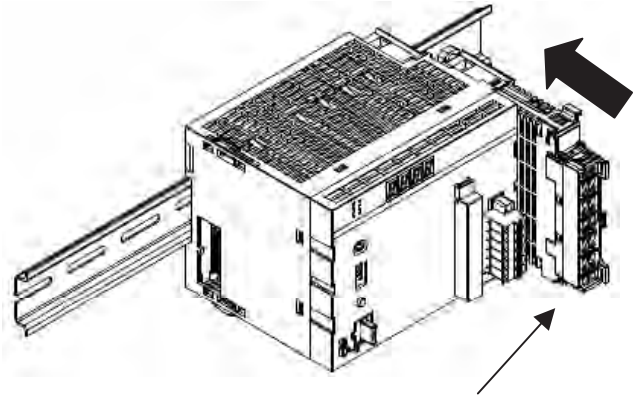
Do not mount the Controller as shown in the following figures.


Up
Up
Down
Down
Up
Up
Down
Down

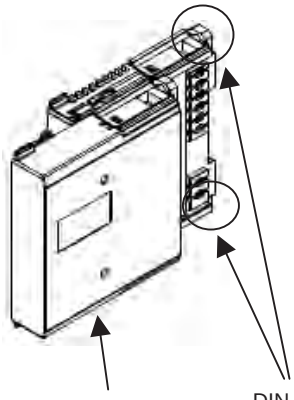
16-1-3 Mounting I/O Units

Connect CPU Units and I/O Units together by sliding the I/O Units in from the front, as shown in the following figure.

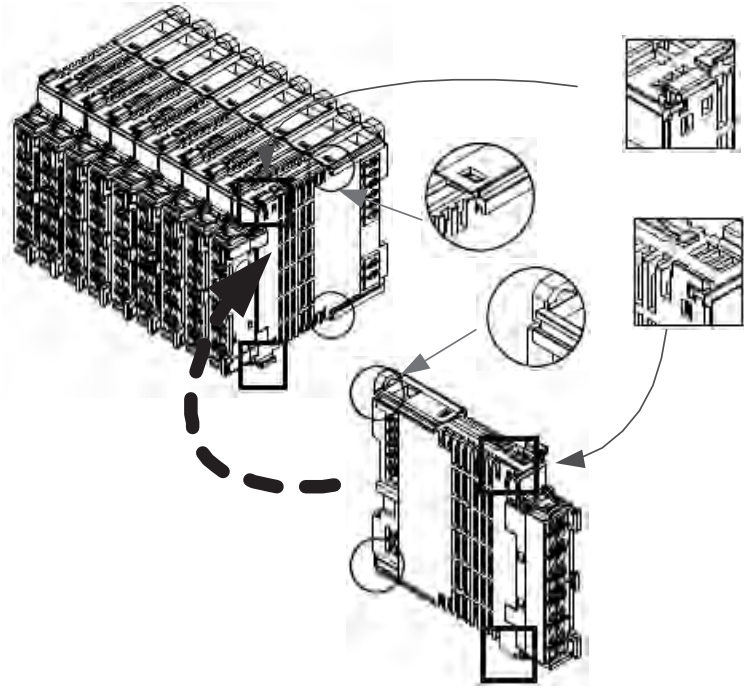
Connect the desired number of I/O Units in order. An End Unit must always be connected to the last I/O Unit.



Slide the Unit and push it against the DIN Track until a clicking sound is heard and the Unit locks in place.
There is no need to release the DIN Track installation hooks before mounting the Unit.



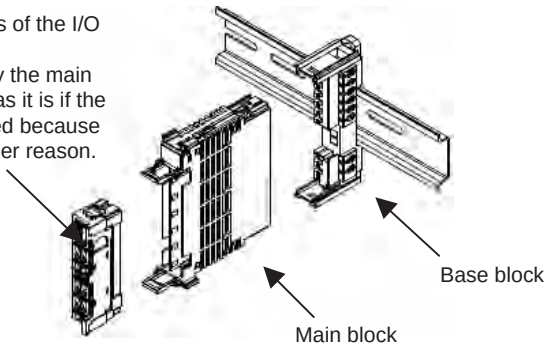
Note When connecting Units, make sure the guides on both Unit mate and then slide the Units together.



I/O Unit Structure

An I/O Unit consists of the following three blocks. Each block can be removed for replacement or other purposes.

Terminal Block
This block has the terminals of the I/O Unit.
It is possible to replace only the main block and leave the wiring as it is if the main block must be replaced because it is damaged or for any other reason.

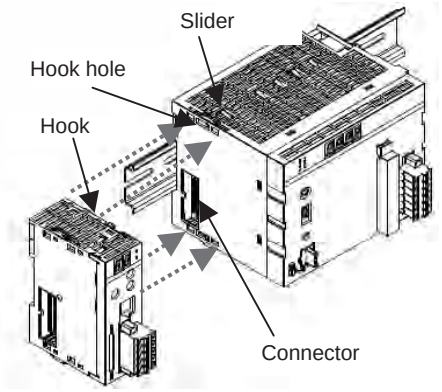


16-1-4 Mounting Communications Units

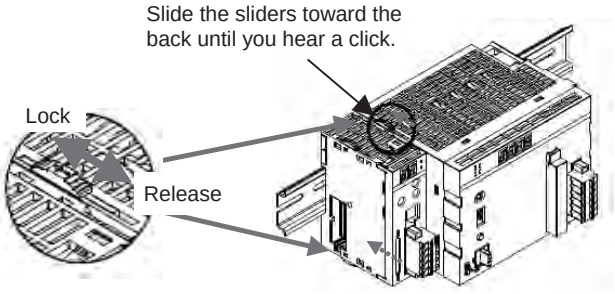
Connect the first Communications Unit to the CPU Unit or connect two Communications Units by connecting the connectors between them and locking the sliders.

Connect an NE2A-TER01 End Cover to the last Communications Unit on the left if power is not connected to the last Communications Unit.

1,2,3... 1. Securely connect the connectors to connect the Units together.



2. Slide the yellow sliders on the top and bottom until they click into place and the Units are locked together.



Be sure to mount a Power Supply Unit to the left end when adding a Communications Unit. Operation will not be performed correctly if a Power Supply Unit is not mounted.

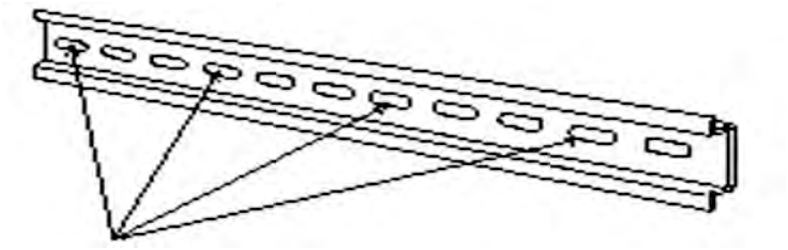
16-1-5 Mounting the DIN Track

Mounting the DIN Track

Mount the NE2A-series Controller Units to a DIN Track.

Mount the DIN Track with screws in every three oval holes (i.e., at a pitch of 105 mm max.).

DIN Track: PFP-50N (50 cm) or PFP-100N (100 cm)

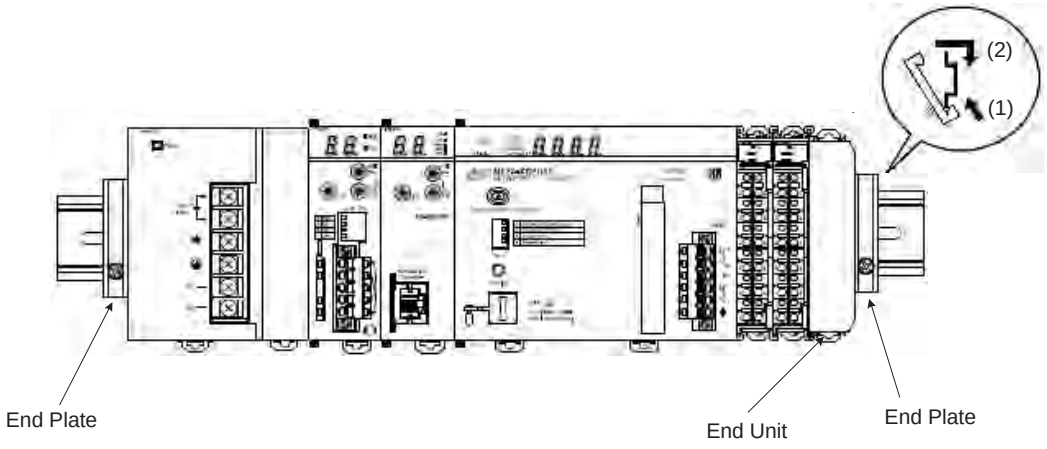


Mount the DIN Track with screws at a pitch of 105 mm max.

Mounting End Plates

Always secure the Units with one PFP-M End Plates on each end.

Hook the bottom of the End Plate on the DIN Track (as shown at 1 in the figure), hook on the top of the End Plate on the DIN Track, and then pull down on the End Plate (as at 2 in the figure). Tighten the screw to secure the End Plate.

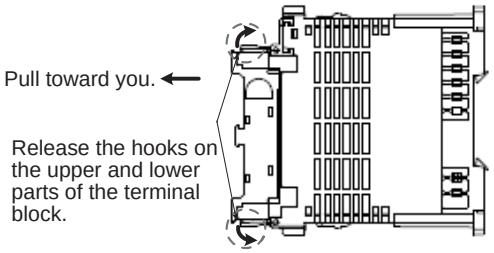


Note Be sure to secure the Controller between two End Plates, one each side.

16-1-6 Removing an I/O Unit

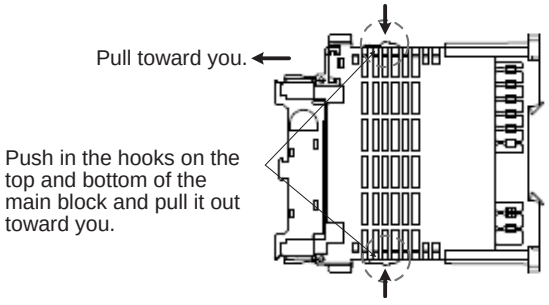
Removing Only the Terminal Block

Release the hooks on the top and bottom of the terminal block and pull out the terminal block.



Removing Only the Main Block

Push in the hooks on the main block and pull the block toward you.

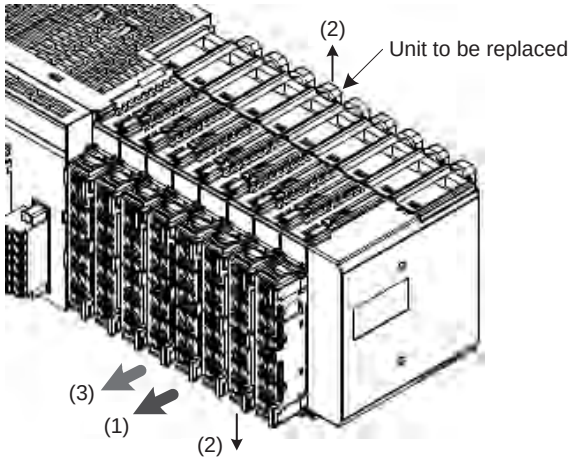


Removing Individual Base Blocks

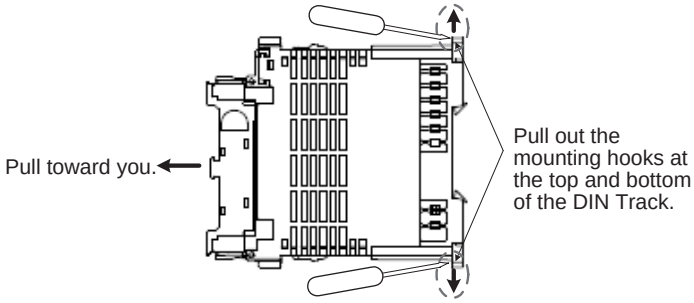
(1) First, remove the main block on the ride side of the I/O Unit to be replaced.

(2) Release the top and bottom hooks holding I/O Unit to be replaced to the DIN Track.

(3) In a straight line, pull out the I/O Unit to be replaced.



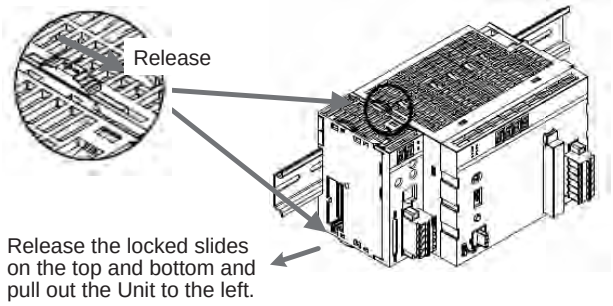
Pull out the top and bottom hooks holding I/O Unit to the DIN Track with a flat-head screwdriver and pull out the Unit in a straight line.



The NE2A-series Controller will not operate normally if a Base Block without a Main Block and Terminal Block is connected.

16-1-7 Removing a Communications Unit

Slide the yellow sliders on the top and bottom until they click to release the lock and then pull out the Unit to the left (i.e., to the side of the Controller).



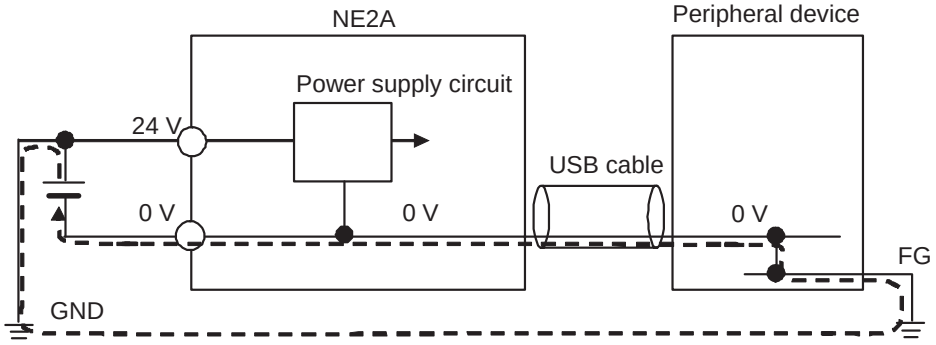
Release the locked slides on the top and bottom and pull out the Unit to the left.

16-2 Wiring

16-2-1 General Precautions and Reference for Performing Wiring

Placement and Wiring

- Always turn OFF the power supply before performing wiring. External devices connected to the NE2A-series Controller may operate unexpectedly.
- Properly apply the specified voltage to the input terminals. Applying an inappropriate DC voltage or any AC voltage will disable the specified functionality, decrease safety functions, damage the product, or result in fire.
- Be sure to separate the communications cables and I/O cables from high-voltage and high-current lines.
- Be careful not to get your fingers caught when attaching the connectors.
- Tighten the DeviceNet connector screws to the specified torque (0.25 to 0.3 N·m).
- Incorrect wiring may lead to loss of safety functions. Wire conductors correctly and verify operation of the NE2A-series Controller before using the system in which the NE2A-series Controller is incorporated.
- After wiring is completed, be sure to remove the label for preventing dust entry to enable proper heat dissipation.



Selecting a Power Supply

Use a DC power supply that satisfies the following requirements.

- The secondary circuits of the DC power supply must be isolated from the primary circuit by double insulation or reinforced insulation.
- The DC power supply must satisfy the output characteristic requirements for class 2 circuits or limited voltage/circuit currents given in UL 508.
- The output hold time must be 20 ms or longer.
- An SELV power supply that satisfies IEC/EN 60950-1 and EN 50178 must be used.

Precautions for Removing Units

- Always turn OFF the power supply before installing or removing Units or attaching wires.
- Wire clippings may become scattered when wiring is performed. Perform wiring with the label attached to the top of the Unit to prevent foreign matter from entering the Unit. After wiring is completed, be sure to remove the label to enable heat dissipation.

16-2-2 Applicable Wire Sizes, Crimp Terminals, and Tightening Torque

CPU Units and I/O Units

This section gives the applicable wire sizes for NE2A-series CPU Units and I/O Units.

Wire Sizes

Refer to the following for wire sizes for wiring the CPU Unit and external I/O devices.

Solid wire	0.2 to 2.5 mm^2 AWG 24 to 12
Stranded wire	0.34 to 1.5 mm^2 AWG 22 to 16

Using Ferrules with Plastic Insulated Covers

Use a ferrule with an insulative cover compliant with DIN 46228-4. Even if the shape is the same, the ferrule may not be applicable to the terminal block if the ferrule does not comply with this standard. (The wire dimensions are rough standards. Confirm the dimensions beforehand.)

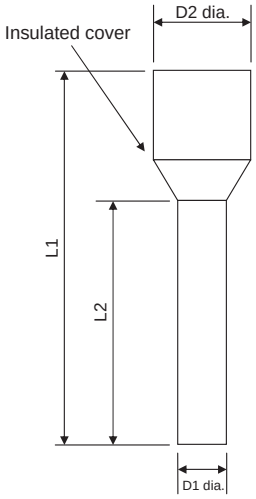
Note

- When wiring with ferrules, be sure to insert the ferrules all the way into the terminal block.
- When using two-wire ferrules, always use wires of the same diameter.
- When using two-wire ferrules, insert the ferrule so that the metal portion of the ferrule is inserted straight into the terminal block, i.e., so that the long sides of the insulative cover are vertical.

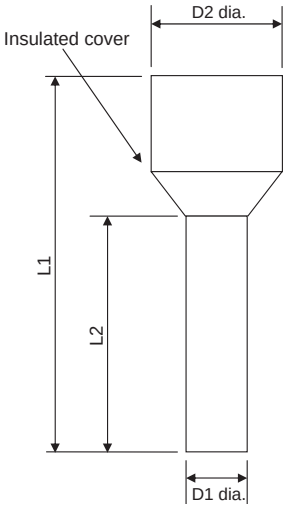
Reference Specifications (Product Specifications for Phoenix Contact)

Model of ferrule		Wire dimensions		Ferrule specifications					Dimensions
		Cross sectional area of conductor (mm^2)	AWG	Stripped length of insulation (mm)	Overall length L1 (mm)	Length of metal part L2 (mm)	Inner diameter of conductor D1 (mm)	Inner diameter of insulative cover D2 (mm)	
One-wire ferrules	AI 0,34-8TQ	0.34	22	10	12.5	8	0.8	2.0	*1
	AI 0,5-10WH	0.5	20	10	16	10	1.1	2.5	
	AI 0,75-10GY	0.75	18	10	16	10	1.3	2.8	
	AI 1-10RD	1.0	18	10	16	10	1.5	3.0	
	AI 1,5-10BK	1.5	16	10	18	10	1.8	3.4	
Two-wire ferrules	AI-TWIN 2 × 0,75-10GY	2 × 0.75	---	10	17	10	1.8	2.8/5.0	*2
	AI-TWIN 2 × 1-10RD	2 × 1	---	10	17	10	2.05	3.4/5.4	

*1 One-wire Ferrule



*2 Two-wire Ferrule



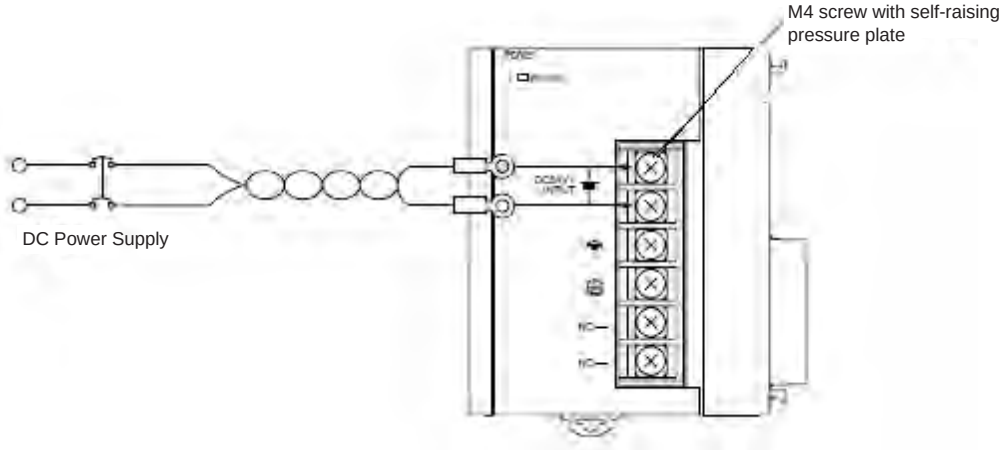
- Terminal Crimping Tool

Manufacturer	Model
Phoenix Contact	CRIMPFOX UD6 or CRIMPFOX ZA3

Note

- Properly apply the specified voltage to the input terminals. Connecting a DC power supply that exceeds the specifications or any AC voltage will disable the specified functionality, decrease safety functions, damage the product, or result in fire.
- Lay the I/O signal cables separated from high-voltage lines and power lines.
- I/O signal cables must be no longer than 100 m.
- Do not apply a power supply to the output terminals. Doing so may damage the product or result in fire.
- Do not apply a power supply to the test output terminals. Doing so may damage the product or result in fire.

Power Supply Unit



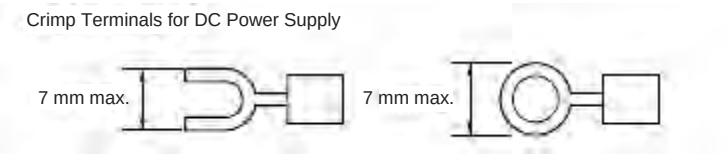
Terminal Screws

M4 screws with self-raising pressure plates are used for the terminal screws on the power supply wiring section.

Note

- Tighten the terminal block screws to a torque of 1.2 N·m.
- Use the following types of crimp terminal for M4 screws.

Crimp Terminals for DC Power Supply



16-2-3 DeviceNet Wiring

Refer to the *DeviceNet Operation Manual* (Cat. No. W267) for information on laying DeviceNet networks.

16-2-4 Ethernet Wiring

Recommended Network Configuration Device

These products are recommended for use with the EtherNet/IP Unit.

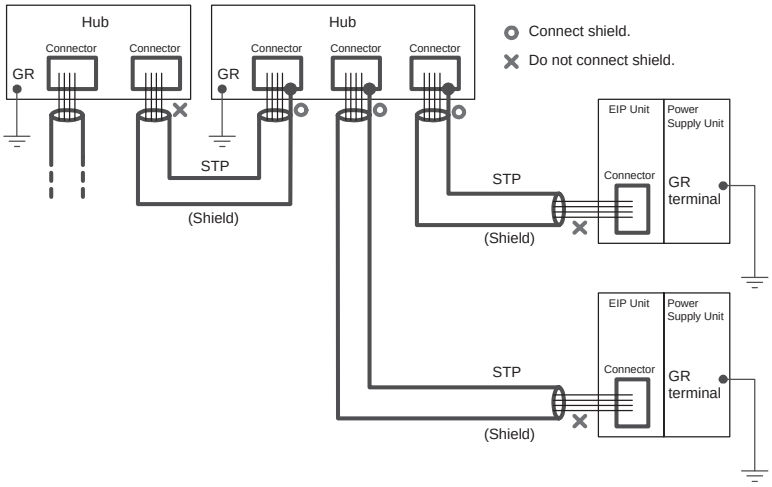
Part	Maker	Model number	Inquires
Switching Hub	Cisco Systems, Inc.	Consult the manufacturer.	Cisco Systems, Inc. Main Corporate HQ
	Contec USA, Inc.	Consult the manufacturer.	CONTEC USA Inc.
	Phoenix Contact	Consult the manufacturer.	Phoenix Contact USA Customer Service
Twisted-pair cable	100BASE-TX		
	Fujikura	F-LINK-E 0.5mm × 4P	Fujikura America, Inc.
	EtherNet/IP compliant cable		---
Connectors (Modular plug)	STP Plug		
	Panduit Corporation	MPS588	Panduit Corporation US Headquarters
Boots	Tsuko Company	MK boot (IV) LB	Tsuko Company Japan Headquarters

Basic Precautions for Laying a Network

- It is necessary to take sufficient safety measures and follow the specifications when performing work to lay an Ethernet network. Refer to JIS X5252 for standards related to laying an Ethernet network and to *Standards for Electrical Equipment and Technology* for performing work to lay networks.
- It is recommended that work for laying the network be performed by a service provider that is familiar with the safety measures and specifications.
- Do not install Ethernet network devices near devices that generate noise. If devices must be installed in an environment that is subject to excessive noise, always take measures against noise, such as by storing each network configuration device in a metal enclosure or using optical cable for part of the system.
- If increased communications traffic can be expected due to Tag Data Links when the EtherNet/IP network is laid together with a data network, it is recommended to make a network configuration that will not be affected, such as by using a separate Ethernet segment for the data for the EtherNet/IP network.

Precautions for Laying Twisted-pair Cable

- The level of noise resistance may decrease due to a grounding loop caused by how the shields are connected or how the devices are grounded. Connect the shields as shown in the following figure, i.e., connect each shield at only one point.
- Do not connect the connector shield on the EtherNet/IP Unit.
- Connect each shield at only one end of the cable that connects two hubs together.

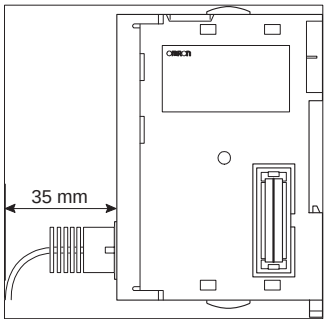


- When connecting to a switching hub or EtherNet/IP Unit, securely insert the connectors until they lock.
- Do not lay the cable together with high-voltage lines.
- Do not lay the cable near devices that generate noise.
- Do not lay the cable in an environment that is subject to high temperatures or high humidity.
- Do not use the cable in locations subject to excessive dust or oil mist.

Connecting the Ethernet Cable

Note

- Turn OFF the power supply to the NE2A-series Controller before connecting or disconnecting the twisted-pair cable.
- Allow enough space for the bending radius of the twisted pair cable as shown in the following figure.



1,2,3...

1. Lay the twisted-pair cable.
2. Connect the cable to the switching hub.

3. Connect the twisted-pair cable to the connector on the EtherNet/IP Unit. Be sure to press the connectors (at both the switching hub and Ethernet) until they lock into place.

16-3 Hardware Settings

Refer to *SECTION 3 Configuration Unit Specifications and Nomenclature* to make the settings with the rotary switches or DIP switches on each Unit.

SECTION 17
Downloading Device Parameters and Operating the Safety Control System

This section describes how to download parameters to the NE2A-series Safety Network Controller system and operate the system.

17-1 Overall Procedure for Downloading Parameters and Operating the Safety Control System 424
17-2 Connecting Online 425
17-2-1 Connecting to a Network through the USB Port 425
17-2-2 Connecting to a Network through an DeviceNet Interface Board . . 426
17-2-3 Connecting to a Network through an Ethernet Port 428
17-2-4 Connected Networks. 430
17-2-5 Changing the Connected Network 431
17-3 Downloading and Uploading Device Parameters 432
17-3-1 Downloading Device Parameters 432
17-3-2 Uploading Device Parameters 436
17-4 Verifying Parameters and Checking Safety Signatures. 439
17-4-1 Verifying Device Parameters 439
17-4-2 Device Properties 442
17-5 Operating the Safety Control System 445
17-5-1 Changing the Device Mode 445
17-6 Protecting Device Parameters 447
17-6-1 Setting Device Passwords 447
17-6-2 Lost Device Passwords 448
17-7 User Test and Automatic Operation 451
17-7-2 Locking Configurations 451
17-7-3 Unlocking the Device Configuration 452
17-8 Resetting Devices 454
17-8-1 Resetting a Device 454
17-8-2 Reset Types and Device Status 455
17-9 Changing Device Parameters and Operating Modes Using a Memory Card . 456
17-9-1 Creating and Checking the Configuration Restore File 456
17-9-2 Validating the Configuration Restore File 458
17-9-3 Downloading Parameters and Locking the Configuration 458
17-9-4 Changing the Operating Mode 461

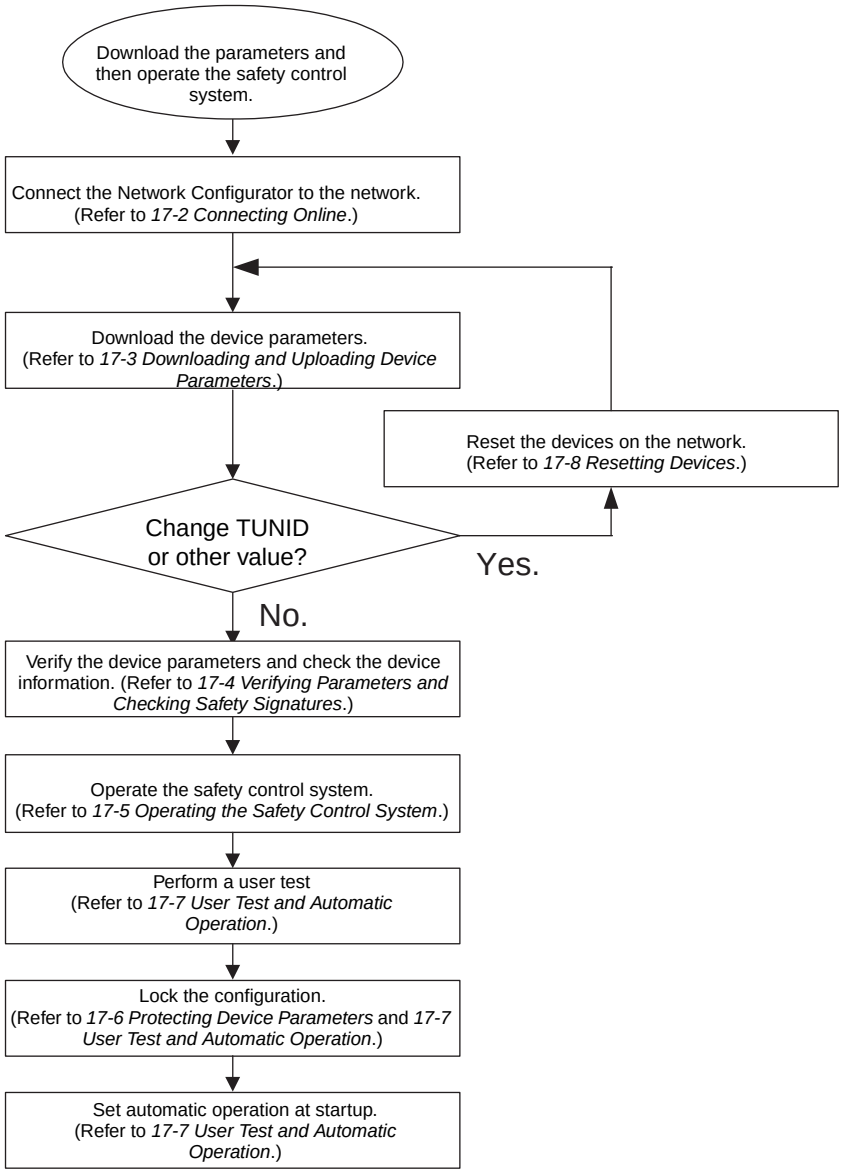
17-1 Overall Procedure for Downloading Parameters and Operating the Safety Control System

This section describes how to download parameters and then operate the safety control system.

Overall Procedure for Downloading Parameters and Operating the Safety Control System

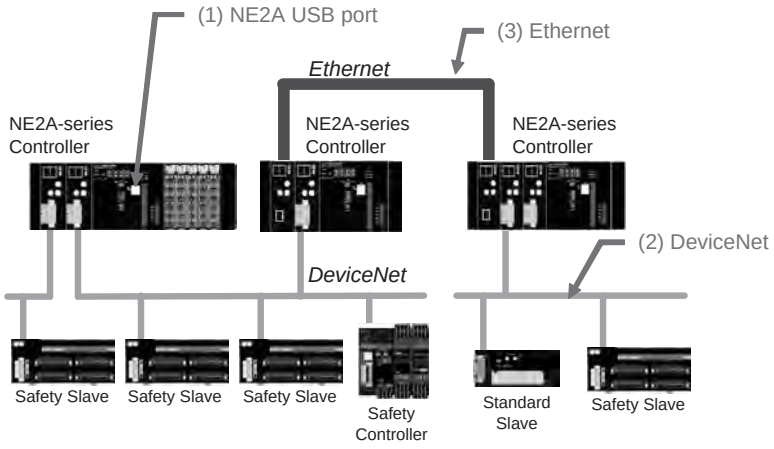
The procedure for connecting the Network Configurator, downloading parameters from the Network Configurator, and then operating the safety control system is described below. With the Logic Editor, you can perform these online operations only for the Safety Controller that is connected online.

Resetting the Safety Devices is not necessary when performing basic operations. However, if you want to change information, such as a TUNID, of a previously configured device, you must reset the Safety Device.



17-2 Connecting Online

This section describes how to connect the Network Configurator to a network.

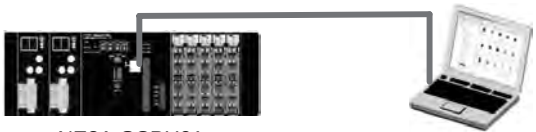


The Network Configurator can be connected to the system shown above in any of the following three ways:

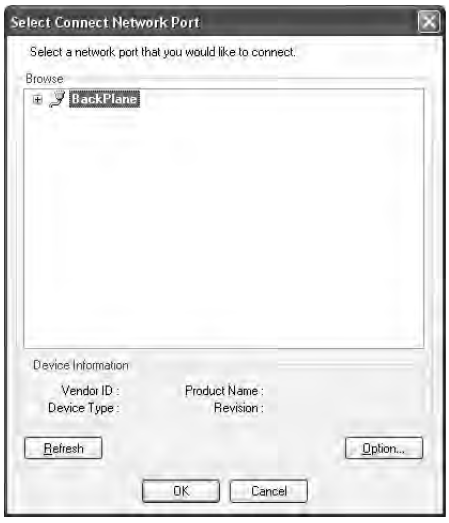
1. Connecting to the USB port of an NE2A-series CPU Unit
2. Connecting to a DeviceNet network by inserting a DeviceNet Interface Board in the computer
3. Connecting to an EtherNet/IP network through the Ethernet port on the computer

17-2-1 Connecting to a Network through the USB Port

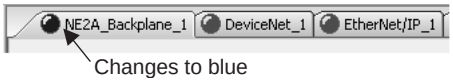
1,2,3... 1. Turn ON the power supply to the NE2A-SCPU01 and connect it to the USB port of the computer.
If the USB driver is not installed on the computer (i.e., if the computer finds new hardware), refer to *9-3 Installing the USB Driver*, and install the USB driver.



2. Select ***Select Interface - NE2A USB Port*** from the Options Menu.
3. Select ***Connect*** from the Network Menu.
You can also right-click the mouse in an open area of the Network Configuration Pane and select ***Connect*** from the pop-up menu.
Or, you can click the **Connect** Icon ( ) in the toolbar.
The Setup Interface Dialog Box will be displayed.
The Select Connect Network Port Dialog Box will be displayed.



4. Select the network to connect to and click the **OK** Button.
When the online connection has been established successfully, the Connected Network Identifier in the Network Configuration Pane will turn blue. (Refer to *9-6-2 Network Configuration Pane*, for details on the Connected Network Identifiers.)



The connection status will change to **On-line** ( ) in the status bar displayed at the bottom of the window. (Refer to *9-6-5 Status Bar*, for details on the connection status.)

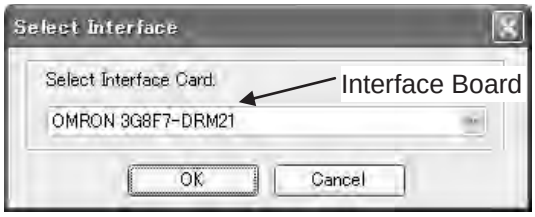


17-2-2 Connecting to a Network through an DeviceNet Interface Board

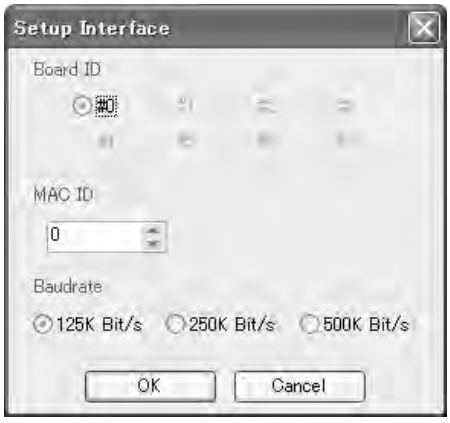
Procedure

1,2,3...

1. Select ***Select Interface - DeviceNet I/F*** from the Options Menu.
2. Select ***Connect*** from the Network Menu.
You can also right-click the mouse in an open area of the Network Configuration Pane and select ***Connect*** from the pop-up menu.
Or, you can click the **Connect** Icon ( ) in the toolbar.
The Select Interface Dialog Box will be displayed.



3. Select the Interface Board and then click the **OK** Button.
The Setup Interface Dialog Box will be displayed.



This dialog box will differ with the Interface Board that is selected. Here, a 3G8F7-DRM21 DeviceNet PCI Board is used as an example. If you are using any other Interface Board, refer to the manual for that board.

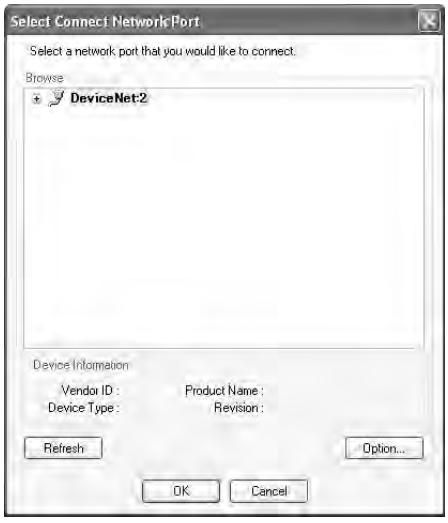
The items specified in the Setup Interface Dialog Box are described in the following table.

Item	Description
Board ID	This is a number that is used to identify the board when more than one DeviceNet Interface Board is inserted in the same computer. You can set any number from 0 to 7, as long each Board is assigned a unique number. (The default setting is 0.)
MAC ID	Select the node ID of the DeviceNet Interface Board.
Baud rate	Select the baud rate of the DeviceNet network to connect to.

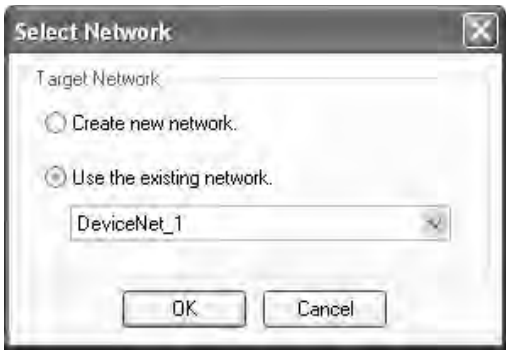
4. Make the settings, and then click the **OK** Button.
   A message box will be displayed to confirm the baud rate.



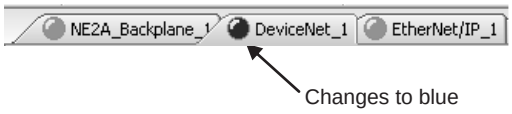
5. Click the **OK** Button.
   The Select Connect Network Port Dialog Box will be displayed.



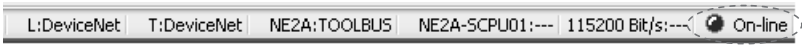
6. Select the network to connect to, and then click the **OK** Button.
The Select Connected Network Dialog Box will be displayed.



7. Select the Target network in the Target Network Area, and then click the **OK** Button.
When the online connection has been established successfully, the Connected Network Identifier in the Network Configuration Pane will turn blue. (Refer to *9-6-2 Network Configuration Pane*, for details on the Connected Network Identifier.)



The connection status will change to **On-line** ( ) in the status bar displayed at the bottom of the window. (Refer to *9-6-5 Status Bar*, for details on the connection status.)



17-2-3 Connecting to a Network through an Ethernet Port

Procedure

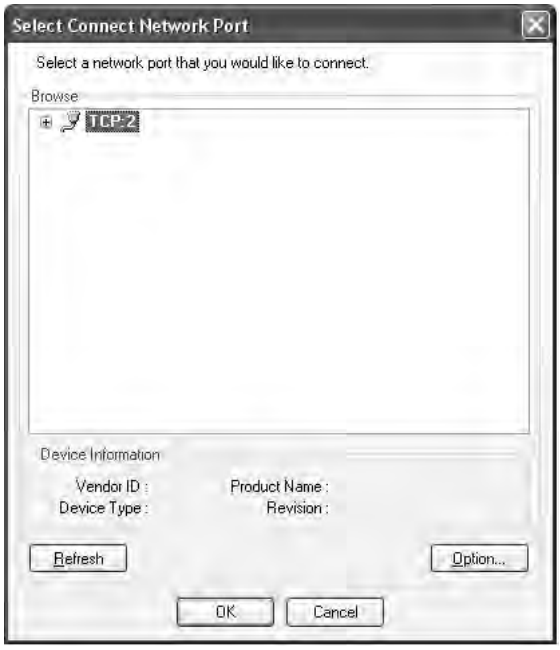
1,2,3...

1. Select ***Select Interface - Ethernet I/F*** from the Options Menu.
2. Select ***Connect*** from the Network Menu.
You can also right-click the mouse in an open area of the Network Configuration Pane and select ***Connect*** from the pop-up menu.
Or, you can click the **Connect** Icon ( ) in the toolbar.

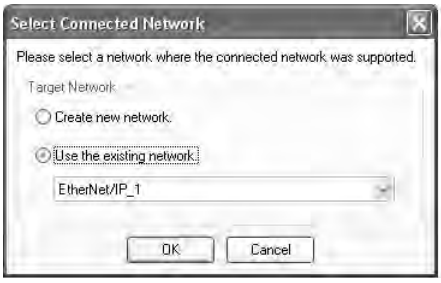
Note The Select Interface Dialog Box will be displayed if multiple computer Ethernet ports are enabled.



3. Select the Ethernet port to connect to, and then click the **OK** Button.
The Select Connect Network Port Dialog Box will be displayed.



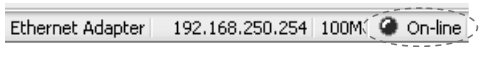
4. Select the network to connect to, and then click the **OK** Button.
The Select Connected Network Dialog Box will be displayed.



5. Select the Target network to connect to and click the **OK** Button.
When the online connection has been established successfully, the Connected Network Identifier in the Network Configuration Pane will turn blue. (Refer to *9-6-2 Network Configuration Pane*, for details on the Connected Network Identifier.)



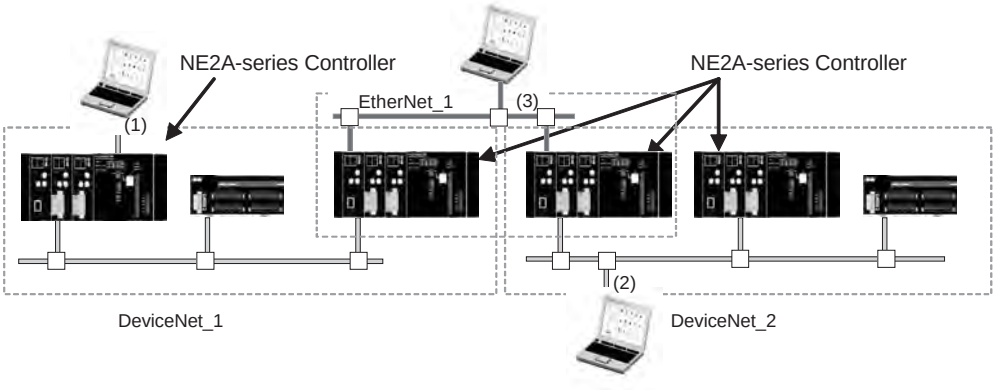
The connection status will change to **On-line** ( ) in the status bar displayed at the bottom of the window. (Refer to *9-6-5 Status Bar*, for details on the connection status.)



17-2-4 Connected Networks

If you use the Network Configurator and an NE2A-series Communications Unit, you can perform online operations, such as uploading and downloading parameters, not only with the connected network, but also with any other networks that the connected device is part of.

A system connected to more than one network (DeviceNet_1, EtherNet_1, and DeviceNet_2), as shown in the following figure, is described below.



Displaying the Network Connection Window

When the Network Configurator is connected to a network, you can identify the online network by the color of the Connected Network Identifier on the Network Configuration Pane.



Color of the Connected Network Identifier	Description
: Gray	The identifier changes to this gray either when the Network Configurator is offline, or when the network is not connected online.
: Blue	Indicates a network to which the Network Configurator is directly connected online.
: Green	Indicates a network that is indirectly connected online via a router device on another online network.
: Red	Indicates the error status of a network.

If you want to communicate (perform operations) with a network whose Connected Network Identifier is gray, you must change the connected network.

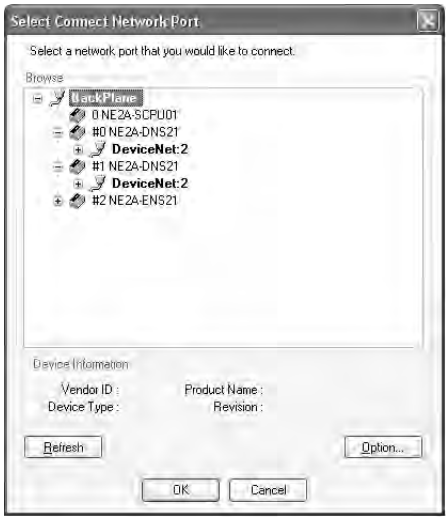
If the identifiers are displayed as shown above, you need to change the connected network from EtherNet/IP to DeviceNet. (Refer to *17-2-5 Changing the Connected Network* for details on how to change the connected network.)

17-2-5 Changing the Connected Network

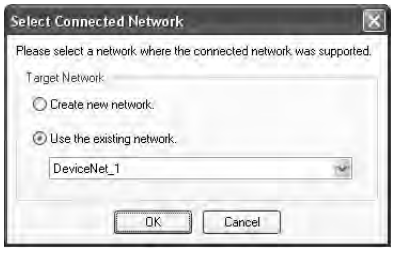
This section describes how to change the connected network.

Procedure

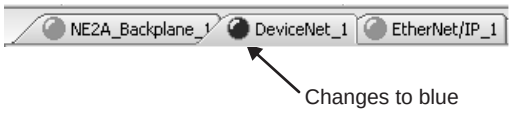
1,2,3... 1. Select ***Change Connect Network*** from the Network Menu.
The Change Connect Network Dialog Box will be displayed.



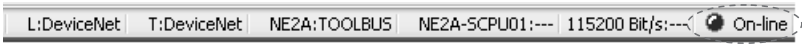
2. Select the network to connect to, and then click the **OK** Button.
The Select Connected Network Dialog Box will be displayed.



3. Select the Target network to connect to, and then click the **OK** Button.
When the online connection has been established successfully, the Connected Network Identifier in the Network Configuration Pane will turn blue. (Refer to *9-6-2 Network Configuration Pane*, for details on the Connected Network Identifier.)



The connection status will change to **On-line** ( ) in the status bar displayed at the bottom of the window. (Refer to *9-6-5 Status Bar*, for details on the connection status.)



17-3 Downloading and Uploading Device Parameters

This section describes how to download and upload parameters to and from network devices. By downloading the parameters, the parameters that have been specified for a particular devices on the Network Configurator can be set up in the physical devices. By uploading parameters, the parameters that have been set up in the physical devices can be read to the Network Configurator.

17-3-1 Downloading Device Parameters

You can download parameters in two ways: downloading to the selected device and downloading to the entire network. Parameters can be downloaded only when the Network Configurator is connected online.

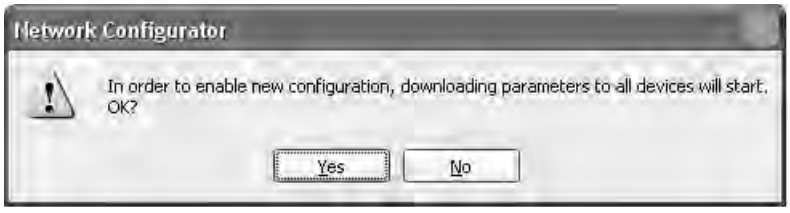
You can perform this operation only for devices present in a network for which the Connected Network Identifier is either blue or green when the Network Configurator is connected to the network. (This does not include when an NE0A-series Controller, NE1A-SCPU01 CPU Unit (Pre-Ver. 1.0), NE1A-SCPU01-V1 CPU Unit, or NE1A-SCPU02 CPU Unit is connected to a USB port.)

Downloading Parameters to Selected Devices

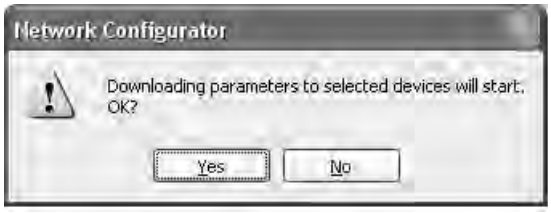
Procedure

1,2,3... 1. Select one or more device in the Network Configuration Pane of the Network Configurator.

2. Select ***Parameters - Download*** from the Device Menu.
   You can also click the **Download to Device** Icon in the toolbar.
   Or, you can right-click the selected device, and select ***Parameters - Download*** from the pop-up menu.
   A dialog box prompting the input of the device password will be displayed.
   - When an NE2A CPU Unit is selected, “all devices” means the NE2A CPU Unit and the Communications Units.



   - If a DST1-series Controller is selected, the following dialog box will be displayed for confirmation.



3. Click the **Yes** Button in the dialog box. A dialog box will be displayed for inputting a password.

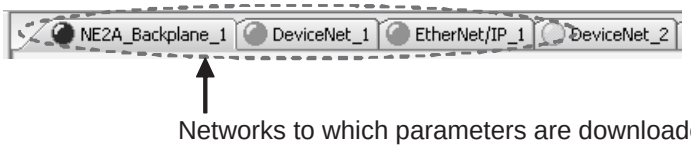


4. Input the device password, and then click the **OK** Button. Downloading will start, and a dialog box for confirmation will be displayed when the downloading has been completed.

Downloading Parameters to All Devices on the Networks (Network Download)

You can download parameters to all devices on the networks currently displayed in the Network Configuration Pane.

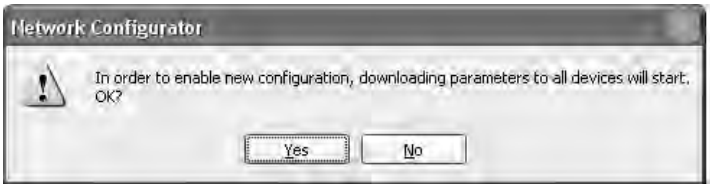
Parameters will be downloaded to all networks for which the Connected Network Identifier is displayed either in blue or green, when the Network Configurator is connected to the network. You can download parameters to all these networks at one time.



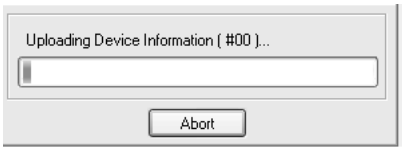
Procedure

1,2,3...

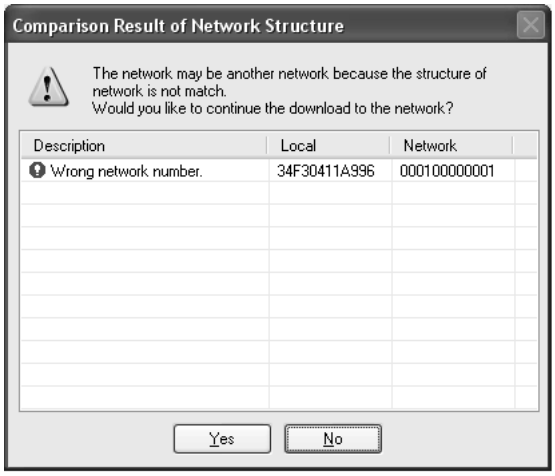
1. Select ***Download*** from the Network Menu.
   You can also right-click the mouse and select ***Download*** from the pop-up menu, when no device has been selected in the Network Configuration Pane.
   Or, you can click the **Download to Network** Icon ( ) in the toolbar.
   A message box will be displayed to confirm downloading to the network.



2. Click the **Yes** Button.
   The Network Configurator will check if its configuration matches the configuration of the actual network.



Note If the network structure does not match, the following dialog box will be displayed.



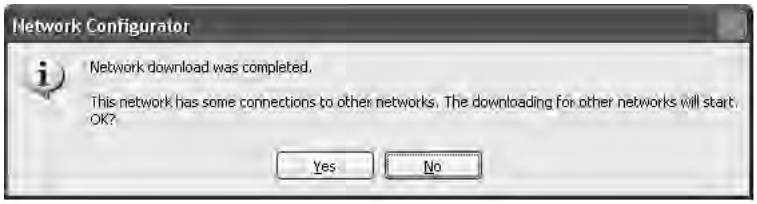
- Click the **No** Button to abort the processing.
- Click the **Yes** Button to start downloading parameters to the network.

  Next, a dialog box prompting the input of the device password will be displayed.

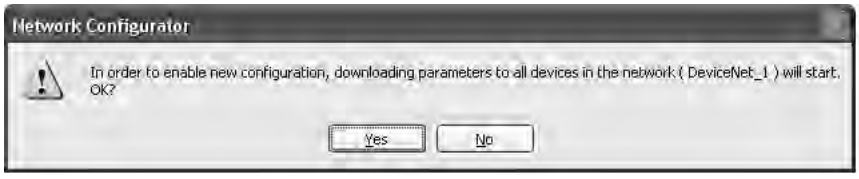


3. Input the device password, and then click the **OK** Button.
   The download will start.

   When the network configuration of one network has been downloaded completely, the following dialog box will be displayed if there are any more networks.



   If you click the **OK** Button, a confirmation dialog box for downloading to another network.



   If you click the **OK** Button, a dialog box to input the device password will be displayed.



If there are multiple devices and the same password is set for all devices, select the *Use this password for all device* Check Box. No further password input will be required.

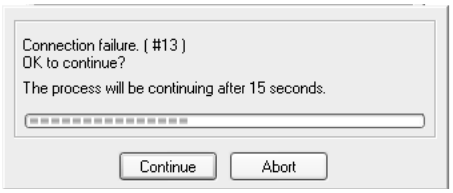
Click the **OK** Button. Downloading to the target network will start.

You can repeat this procedure to download the network configuration to all related networks.

Note After the device parameters have been downloaded, verify them and check that the parameters saved in the devices and the safety signatures are correct.

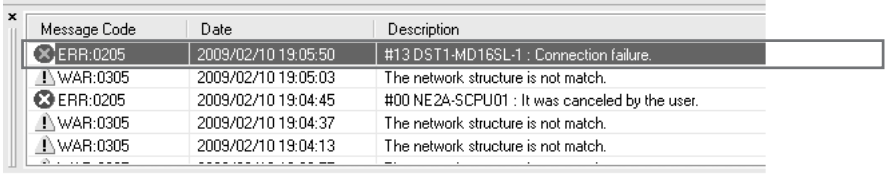
Errors during Downloading

If an error occurs while downloading the configuration to multiple devices one after the other, the following dialog box will be displayed.



Even if you do not click any button and wait in this condition, the processing for the next device will start after 15 seconds. If you click the **Continue** Button, the parameters of the next device will be downloaded. If you click the **Abort** Button, the download process will stop there, and parameters will not be downloaded to any more devices.

Along with the display of the error in the Message Report Pane, the devices in which an error occurred will be listed in the Error Device List Dialog Box.





The errors that occurred while parameters were being downloaded are displayed in the Error Device List Dialog Box for each device.

Note

(1) Refer to *SECTION 19 Troubleshooting* for details and countermeasures of errors other than those discussed above.

(2) The time required to download parameters may be longer if the NE2A-series Safety Master is in RUN Mode. The time required to download parameters can be reduced by changing to IDLE Mode.

17-3-2 Uploading Device Parameters

You can upload parameters in two ways: uploading from the selected device and uploading from the entire network. Parameters can be uploaded only when the Network Configurator is connected online.

You can perform this operation only for devices present in a network for which the Connected Network Identifier is either blue or green when the Network Configurator is connected to the network. (This does not include when an NE0A-series Controller, NE1A-SCPU01 CPU Unit (Pre-Ver. 1.0), NE1A-SCPU01-V1 CPU Unit, or NE1A-SCPU02 CPU Unit is connected to a USB port.)

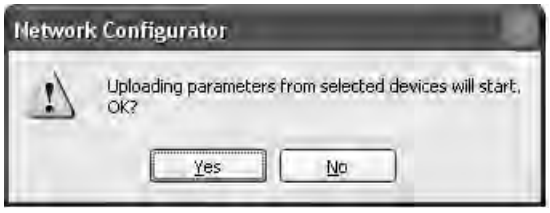
Note If there is a CS/CJ-series DeviceNet Unit on a network, upload parameters after stopping the Master in the CS/CJ-series DeviceNet Unit, or stopping I/O communications from the Monitor Window of the DeviceNet Unit. If the I/O communications are being performed, you may not be able to upload parameters properly.

Uploading Parameters from Selected Devices

Procedure

1,2,3...

1. Select one or more devices from which parameters are to be uploaded in the Network Configuration Pane of the Network Configurator.
2. Select ***Parameters - Upload*** from the Device Menu.
   You can also right-click the device and select ***Parameters - Upload*** from the pop-up menu.
   Or, you can click the **Upload from Device** Icon ( ) in the toolbar.
   A message box will be displayed to confirm starting the upload.

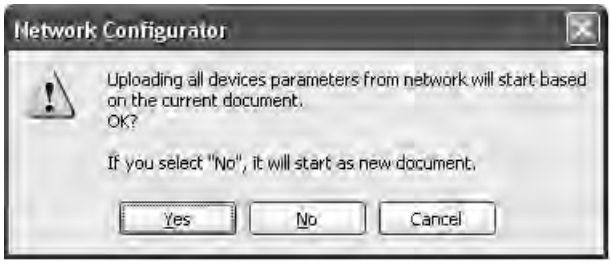


3. Click the **Yes** Button.
   The upload will start.
   When all parameters have been uploaded, a message box will be displayed to indicate the completion of the upload.
4. Click the **OK** Button.
   The process of uploading parameters from the device will end.

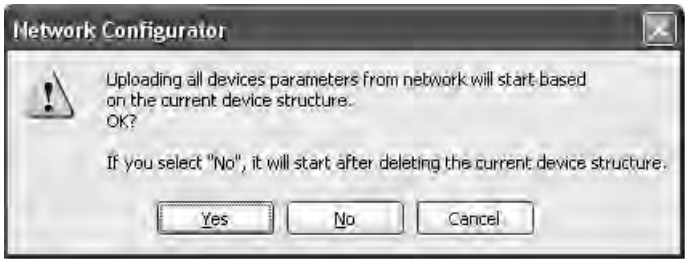
Uploading Parameters from All Devices on the Networks (Network Upload)

Procedure

1,2,3... 1. Select ***Upload*** from the Network Menu.
   You can also right-click the mouse in an open area of the Network Configuration Pane and select ***Upload*** from the pop-up menu.
   Or, you can click the **Upload from Network** Icon ( ) in the toolbar.
   A message box will be displayed to confirm starting the upload.



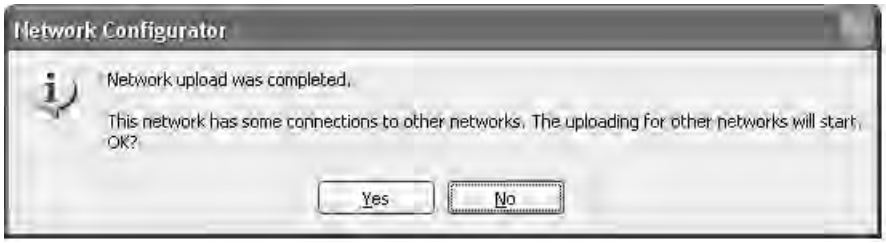
2-1. Click the **Yes** Button.
   A message box will be displayed to re-confirm starting the upload.



- Click the **OK** Button.
  Uploading will start with the displayed Network Configurator device configuration.
- Click the **No** Button.
  The displayed Network Configurator device configuration will be deleted, and uploading will start.
  If the uploading is completed successfully, the parameters can be uploaded with the actual network device configuration.

2-2. Click the **No** Button.
   The following dialog box will be displayed for confirmation if the project has not been saved after being changed.
   If the project has been saved, uploading will start.

3. When uploading for one network has been completed, the following dialog box will be displayed for confirmation if there are related networks.



4. Click the **Yes** Button or the **No** Button.
   When uploading has been completed, a message box will be displayed to indicate the completion of uploading.



5. Click the **OK** Button.
   Uploading from the network will be completed.

17-4 Verifying Parameters and Checking Safety Signatures

This section describes the procedure for checking if the device parameters match the parameters in the Network Configurator.

⚠ WARNING

Serious injury may possibly occur due to loss of required safety functions. Be sure to sufficiently check all parameters related to safety functions.

17-4-1 Verifying Device Parameters

After downloading parameters to one or more devices, verify the parameters. Parameters can be verified only when the Network Configurator is connected online. In the Network Configurator, you can select multiple devices and verify them at the same time.

Procedure

1,2,3...

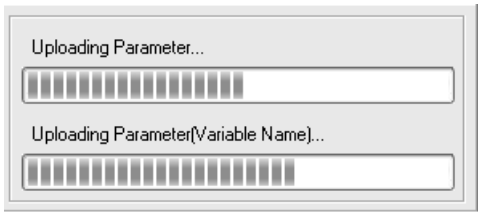
1. Select one or more devices in the Network Configuration Pane of the Network Configurator.

   Hold down the Shift Key when selecting more than one device.

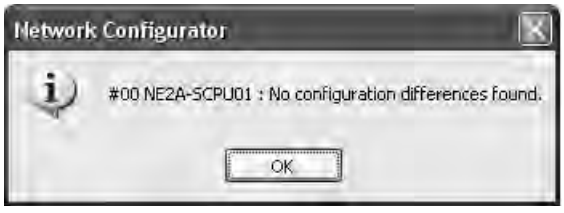
2. Select ***Parameters - Verify*** from the Device menu.
   You can also right-click the device and select ***Parameters - Verify***.

   Or, you can click the **Verify Parameters** Icon ( ) in the toolbar.
   The following confirmation message box will be displayed.

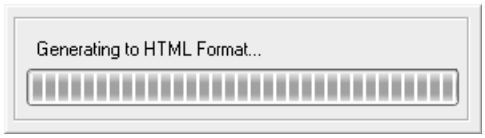
3. Click the **Yes** Button.
   The device parameters will be uploaded.



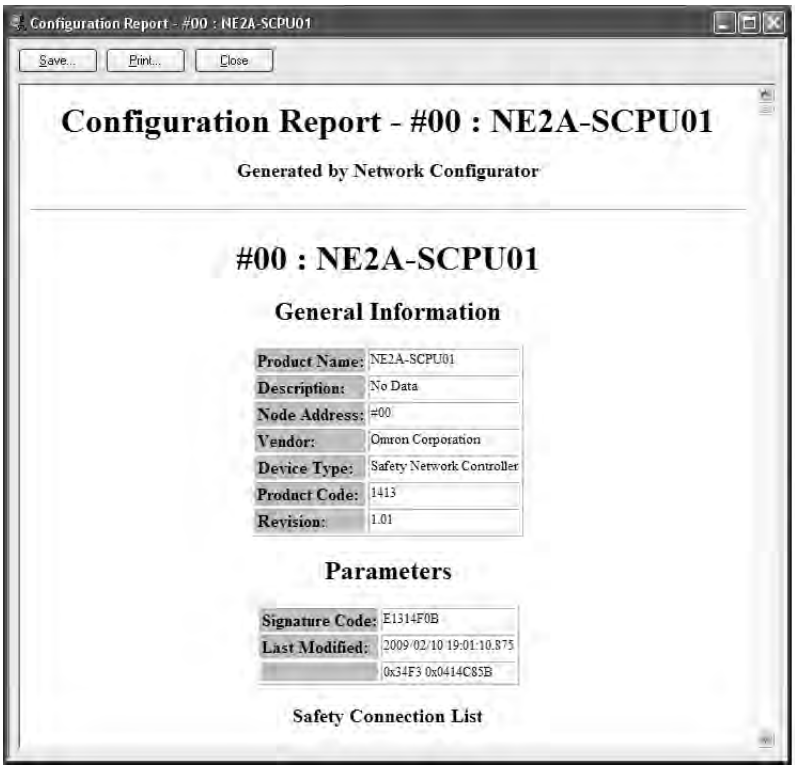
The Network Configurator will check if there are any differences between the parameters registered on the virtual network and the uploaded parameters. If there are no differences, the following dialog box will be displayed.



4. Click the **OK** Button. A message box will be displayed to indicate the progress of conversion to HTML.



After the HTML data is created, the uploaded parameters will be displayed.

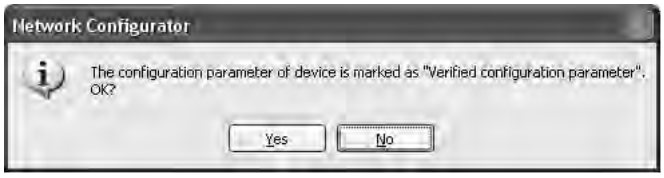


You can check all displayed parameters and confirm if they match the input values.

Note

- You can save the results of verification. To save the results, click the **Save** Button at the top left of the window.
- You can also print the displayed parameters and logic. To print, click the **Print** Button.
- The displayed parameters may not fit into the specified size during printing. If this occurs, edit the saved file with software for editing HTML files, and then print it.

5. After checking the parameters, click the **Close** Button at the top left of the window and close the window.
   The following message box will be displayed.



6. If the parameters matched, click the **Yes** Button.
   The safety mark displayed next to the device icon on the virtual network will turn green to indicate that the configuration has been verified.



After verification, the following message box will be displayed.



7. Click the **Yes** Button. A dialog box will appear to enter the password.
8. Enter the password and click the **OK** Button. The safety mark displayed next to the device icon on the virtual network will change to a mark indicating that the configuration is locked.



Note

- Make sure to save the network configuration file after verifying the parameters of all devices.
- The mark indicating that the configuration is verified shows that the device parameters saved in the network configuration file are correct. This information is saved in the network configuration file, but not in the device itself. Therefore, even when the network configuration is obtained from a verified device by uploading it from the network, the mark indicating that the configuration has been verified will not appear.
- If you edit the parameters of a device whose configuration has been verified, the verification mark will be removed. You will have to verify the parameters of that device again.

When Parameters Do Not Match

If the Network Configurator detects parameters that do not match during verification of parameters, the mismatching parameters will be displayed along with the safety signature in a window like the one shown below. Check the values of the parameters and download these parameters again.



17-4-2 Device Properties

You can check the device information, Safety I/O, Standard I/O, and safety signature in the Device Property Dialog Box.

You can also check the general properties, Safety I/O information, and signature of an NE2A-SCPU01 CPU Unit, and you can check the general properties and I/O information of an NE2A-DNS21 DeviceNet Unit and NE2A-ENS21 Ethernet Unit in the Device Property Dialog Box.

Procedure

1,2,3...

1. Select the NE2A-SCPU01, NE2A-DNS21, or NE2A-ENS21 whose properties are to be displayed.
2. Select ***Property*** from the Device Menu.
   You can also right-click the NE2A-SCPU01, NE2A-DNS21, or NE2A-ENS21 and select ***Property*** from the pop-up menu.
   Or, you can click the **Device Property** Icon ( ) in the toolbar.

Each tab page displayed in the Device Property Dialog Box is described below.

General Tab Page

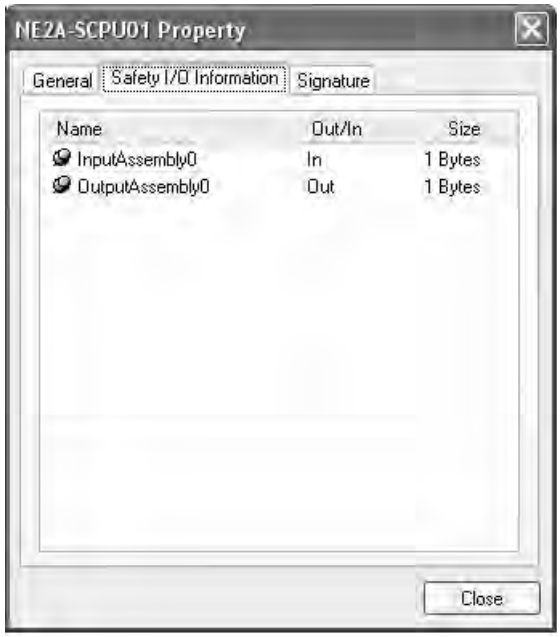
The General Tab Page lets you check the device information and change the device icons displayed in the Network Configuration Pane.



If you click the **Sync** Button, the device information will be obtained from the device and displayed.

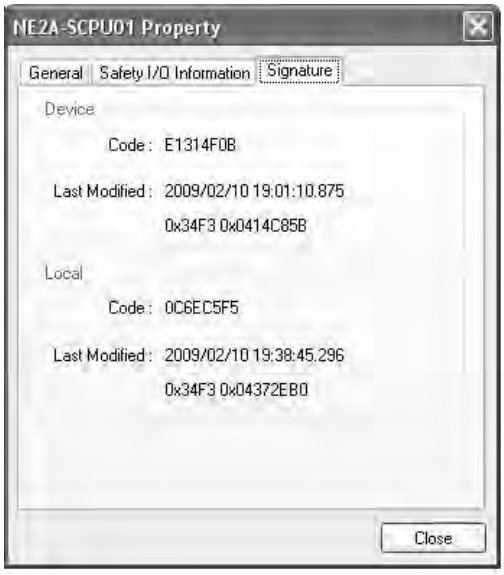
Safety I/O Information Tab Page

The Safety I/O Information Tab Page lets you check the type of the Safety I/O information (I/O assemblies) of the device.



Signature Tab Page

The Signature Tab Page lets you check the safety signature generated by the Network Configurator in the Local Area, and the safety signature of the actual device in the Device Area.



17-5 Operating the Safety Control System

This section describes how to change the device mode to operate the safety control system. With an NE2A-series Controller, you can switch between the IDLE Mode and RUN Mode.

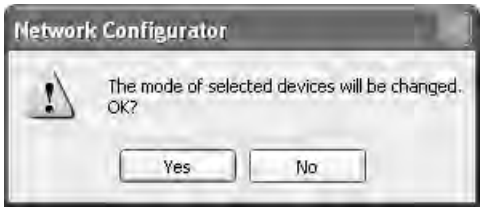
17-5-1 Changing the Device Mode

The device mode can be changed only when the Network Configurator is connected online. With the Network Configurator, you can select more than one device and change their mode at the same time.

Procedure

1,2,3...

1. Select one or more devices for which the operating mode is to be changed.
2. Select ***Change Mode*** from the Device Menu, and then select the mode to be changed.
   You can also right-click the selected device and select ***Change Mode*** from the pop-up menu, and then select the desired mode.
   A dialog box will be displayed to confirm changing the mode.

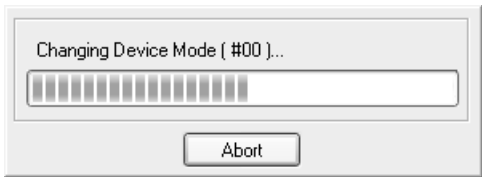


3. Click the **Yes** Button.
   A dialog box prompting the input of the device password will be displayed.

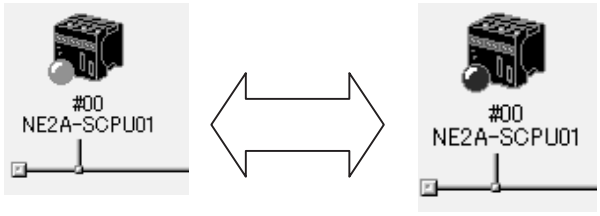


4. Input the password of the Target device and click the **OK** Button.
   If you select more than one device in step 1, the *Use this password for all device* Check Box will be enabled.
   If you select the *Use this password for all device* Check Box, you can use the same password to check all devices.

   The process for changing the device operating mode will start and the following dialog box will be displayed.



IMPORTANT The **Status** Icon in the Maintenance Mode of the Network Configuration Pane can be used to check the operating mode. It will be green in IDLE Mode and blue in RUN Mode.



IDLE Mode RUN Mode

17-6 Protecting Device Parameters

You can protect the parameters and status of Safety Devices from unintentional changes by setting device passwords. This section describes how to set device passwords as a measure for protecting device parameters. A Safety Device will save the password internally.

17-6-1 Setting Device Passwords

You will be prompted to input the device password from the Network Configurator when performing the following operations for a device on a network. You will not be able to execute any of these operations if the password is not correct.

- Downloading to the network
- Downloading parameters
- Locking the configuration
- Unlocking the configuration
- Resetting
- Changing the status
- Changing the password

You can set a password for each device by using the following procedure. Passwords can be set only when the Network Configurator is connected online.

Procedure

1,2,3...

1. Select one or more devices for which a password is to be set.
2. Select ***Change Password*** from the Device Menu.
   You can also right-click a device and select ***Change Password*** from the pop-up menu.
   The Change Password Dialog Box will be displayed.



3. Input the current password and the new password, and then click the **OK** Button.
   You can specify a password between 6 to 16 alphanumeric characters.
   Device passwords are not saved in the network configuration file.

No password is specified for devices in the default settings. If you specify *Return to the default configuration* when resetting a device, you can return to the default configuration in which no password is set. However, you must have the current password to reset the device configuration. Take adequate measures so that you do not lose the device passwords.

Note (1) From the viewpoint of security, it is recommended that passwords be set for all devices.

(2) If you want to set the same password for more than one device, you can specify the setting for using the password for all devices. Select the *Use this password for all device* Check Box in the dialog box prompting to input the device password to use the same password for all devices.



17-6-2 Lost Device Passwords

If you lose the device password, contact your OMRON representative for a recovery key. You must provide the following information to obtain the recovery key. You can also use the Password Recovery Tool to acquire the lost password from the device.

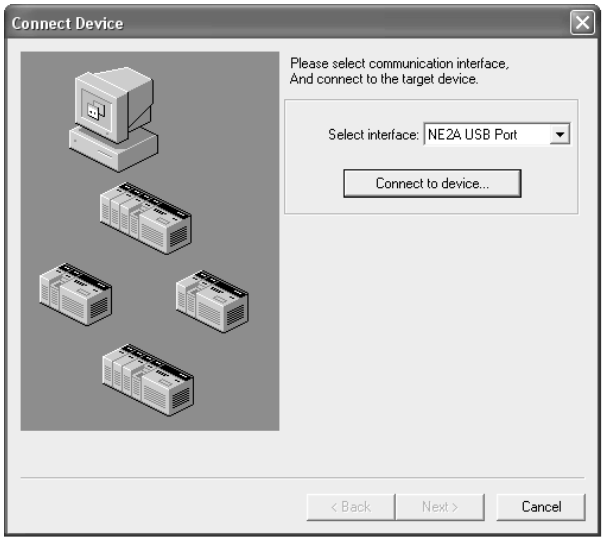
- Vendor ID
- Serial number
- Counter information

You can use the recovery key with the Password Recovery Tool to return the device to the default settings, in which no password is set.

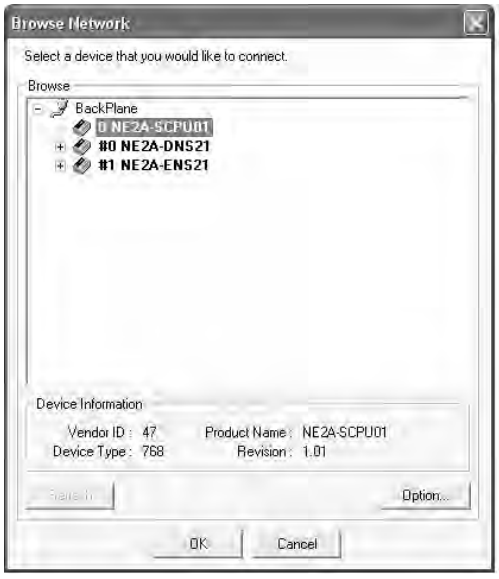
Procedure

1,2,3... 1. End the Safety Network Support Software from the computer.

2. Select ***All programs - OMRON Network Configurator for CIP Safety - Password Recovery Tool*** from the Windows Start Menu.
   The Connect Device Dialog Box will be displayed.



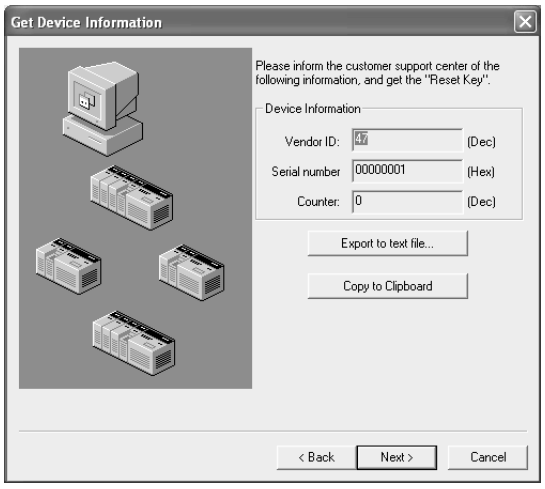
3. Select the interface to which the computer is connected from the Select Interface Field (*NExA USB Port* for a USB port), and click the **Connect to Device** Button.
   When the device has been connected successfully, the Browse Network Dialog Box will be displayed.



   If you fail to connect the device to the interface, the following error message will be displayed.

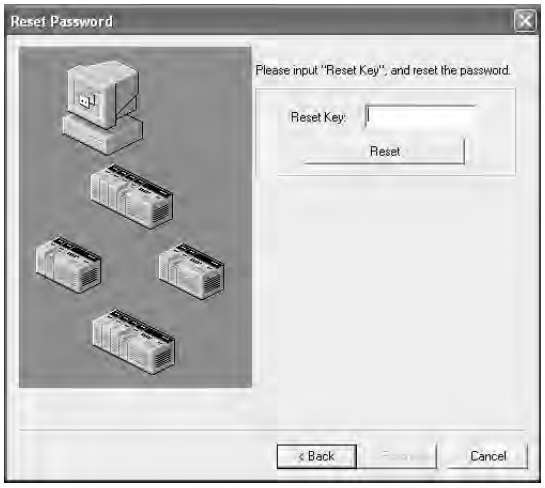


4. Select a device in the dialog box, and then click the **OK** Button.
The Get Device Information Dialog Box will be displayed.



Contact the Support Center with the values displayed here under the Device Information Area for vendor ID, serial number, and counter to obtain the reset key.

5. Click the **Next** Button. A dialog box prompting the input of the reset key will be displayed. Input the number of the reset key obtained from your OMRON representative and click the **Reset** Button.



6. If you have successfully reset the password, the following dialog box will be displayed. This dialog box indicates that the device is now set to the default settings, in which no device password is specified. Click the **OK** Button to close the dialog box, and then exit the Password Recovery Tool Window by clicking the **End** Button.



17-7 User Test and Automatic Operation

This section describes performing a user test, the settings for locking device parameters to protect the safety control system from unintentional changes, and starting operation automatically by turning ON the power.

17-7-1 User Test

In this step, the user himself confirms the program operation and performs functional tests.

Always perform the user test, because it is the user's responsibility to verify the system operation. The user test verifies the correctness of all parameters downloaded to each safety device, as well as each device's safety signature. To demonstrate that all parameters and safety signatures are correct after completing the user test, perform a Configuration Lock operation on all of the safety devices.

⚠ WARNING

Safety functions may be impaired and serious injury may occasionally occur. Before operating the system, perform user testing to confirm that the configuration data of all the devices is correct and that they are operating correctly.



IMPORTANT

- After configuring all the devices, user testing must be performed to check if the configuration data and device operation of each device are correct. User testing is performed to verify the safety signature for each device.
- The configuration must be locked after the user testing has completed.

17-7-2 Locking Configurations

When developing a safety control system, user tests are performed after verifying device parameters. If the operation of a device is confirmed by user tests, it means that the device parameters have been verified by the user.

To protect the verified parameters of a device from unintentional changes, you can lock the configuration.

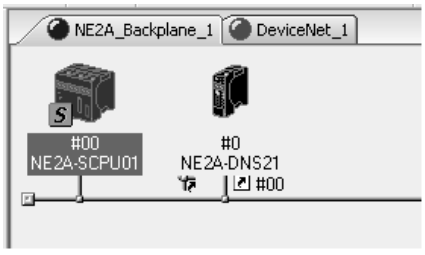
Locking the Device Configuration

The device configuration can be locked only when the Network Configurator is connected online. You can lock the configuration only for a device that has been verified.

Refer to *17-4-1 Verifying Device Parameters* for information of verifying devices.

Procedure

1,2,3... 1. Select one or more devices in the Network Configuration Pane of the Network Configurator.

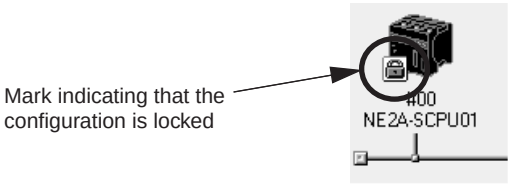


2. Select ***Parameters - Lock*** from the Device Menu.
   You can also right-click the selected device, and select ***Parameters - Lock*** from the pop-up menu.
   A dialog box prompting the input of the device password will be displayed.



3. Input the password of the Target device and click the **OK** Button.
   If more than one device is selected and the same device password is set for all devices, select the *Use this password for all device* Check Box to avoid being prompted to input the password again.

When the configuration has been locked, the safety mark displayed next to the device icon on the virtual network will change to the lock mark, indicating that the configuration is locked.



Note

- Lock the device configuration after performing user tests.
- Make sure to save the network configuration file after locking the configuration of all devices.
- The mark indicating that the configuration is locked means that the device has been tested. This information is not just saved in the network configuration file, but also in the device itself.
- If you lock the configuration, you will not be able to download parameters to that device. To change parameters, you must unlock the configuration.
- If you edit the parameters of a device whose configuration has been verified, the verification mark will be removed. You will have to verify the parameters of that device again.

17-7-3 Unlocking the Device Configuration

To change the parameters of a device whose configuration is locked, you must unlock the configuration. The device configuration can be unlocked only when the Network Configurator is connected online.

Procedure

1,2,3...

1. Select one or more devices in the Network Configuration Pane of the Network Configurator.
2. Select ***Parameters - Unlock*** from the Device Menu.
   You can also right-click the selected device, and select ***Parameters - Unlock*** from the pop-up menu.
   A dialog box prompting the input of the device password will be displayed.

3. Input the device password, and then click the **OK** Button.
   When the configuration has been unlocked, the safety mark displayed next to the device icon on the virtual network will change back to the mark indicating that the configuration is verified.

17-7-4 Automatic Operation at Startup

It is possible to have the system automatically enter RUN Mode to automatically execute the program the next time that the power supply is turned ON when the power supply has been turned OFF with configuration-locked devices in the RUN Mode.

The following conditions apply to starting in RUN Mode when the power supply is turned ON.

- Devices must be locked.
- The operating mode before turning OFF the power supply must be RUN Mode.

Note If you change the device parameters after unlocking the configuration, make sure to lock the configuration again after verifying the parameters.

IMPORTANT The slave input signals can be reflected in the program when the program is executed automatically by enabling the program execution delay. Refer to *4-2-2 Setting NE2A-series Operation at Startup*.

17-8 Resetting Devices

You may not be able to reconfigure a device because information, such as the TUNID, is recorded in a device that has been configured. You must therefore reset the device to its default settings.

This section describes how to reset Safety Devices.

17-8-1 Resetting a Device

You can reset a device by using the following procedure. A device can be reset only when the Network Configurator is connected online.

Procedure

1,2,3...

1. Select one or more devices in the Network Configuration of the Network Configurator.
2. Select ***Reset*** from the Device Menu.
   You can also right-click the device and select ***Reset*** from the pop-up menu.
   The Reset Device Dialog Box will be displayed.

   The Reset Device Dialog Box for a CPU Unit is shown below.



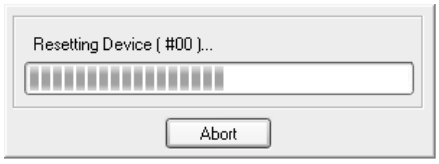
   The Reset Device Dialog Box for a Communications Unit is shown below.



   Refer to *4-2-1 Resetting*, for details on the reset types.

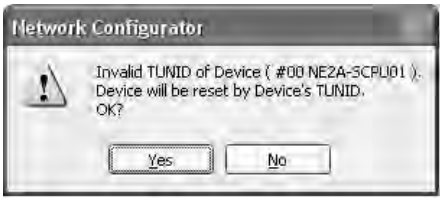
3. Specify the reset type and password, and then click the **OK** Button.
   If you select more than one device in step 1, the *Use this password for all device* Check Box will be enabled. If you select the *Use this password for all device* Check Box, you can use the password to check all devices.

   The following dialog box will be displayed and the reset process will start.



   The reset has been completed when the dialog box shown above closes.

   If the TUNIDs of the Network Configurator and device do not match, the following message box will be displayed. Check if the selected device is the device to be reset and click the **Yes** Button if you want to proceed with the reset process.



⚠ WARNING

Before connecting a device to the network, make sure to clear the previous configuration data. Failure to do so may lead to loss of safety functions, possibly causing serious human injury.

17-8-2 Reset Types and Device Status

Depending on the reset type and the device status, resetting may not be possible.

Reset type	Device status			
	Safety Connection not established		Safety Connection established	
	Configuration unlocked	Configuration locked	Configuration unlocked	Configuration locked
Emulate cycling power	Able to reset	Able to reset	Able to reset*1	Able to reset*1
Return to the default configuration, and then emulate cycling power		Not able to reset		Not able to reset
Return to the default configuration except to preserve the following parameters, and then emulate cycling power				

*1 Stopping Safety I/O Communications is checked to check safety when the reset is executed.



17-9 Changing Device Parameters and Operating Modes Using a Memory Card

It is possible to set parameters, lock the configuration, and change the operating mode of CIP-compatible safety devices on the DeviceNet network of a NE2A-series Controller by inserting a Memory Card that contains a configuration restore file.

17-9-1 Creating and Checking the Configuration Restore File

A configuration restore file is a file that contains the execution rights and system project data used when the system status is changed with a Memory Card of the NE2A-series Controller. Create the configuration restore file by using the Network Configurator to read a project file that was previously created. For the project file, it is recommended that user testing be completed, that safety has been confirmed, and that all devices have been locked.

Creating the Configuration Restore File

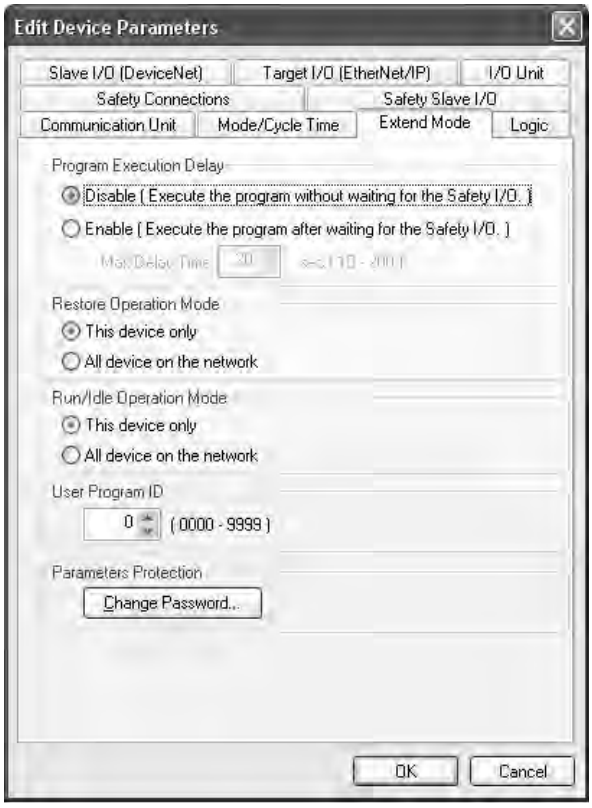
Download the parameters, lock the configuration, select the items for which the operating mode will be changed, and create the configuration restore file.

Procedure

Creating the Configuration Restore File

1,2,3...

1. Select the NE2A-series Controller to execute the process operations, and then select ***Parameter - Edit*** from the Device Menu.
2. Click the **Extend Mode** Tab in the Edit Device Parameters Dialog Box.



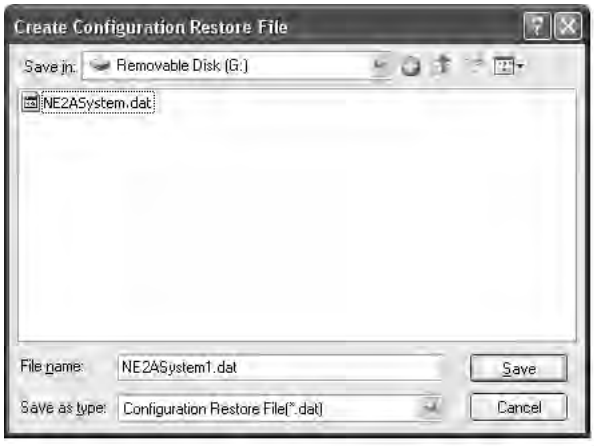
3. Select the devices on which the operations will be performed in the *Restore Operation Mode* Field and *Run/Idle Operation Mode* Field, and then click the **OK** Button.

	This device only	All devices on the network
Restore Operation Setting	Target the relevant NE2A-series Controller and devices with connections to be set with the relevant NE2A-series Controller. Note: Connections in which the NE2A-series Controller is the Master.	Target the safety devices on the DeviceNet network of the NE2A-series Controller. Refer to *7-2 Operation and Maintenance Using a Memory Card*.
RUN/IDLE Operation Setting	Target the relevant NE2A-series Controller.	Target the safety devices on the DeviceNet network of the NE2A-series Controller.

Next, create the configuration restore file for the devices in the targeted range.

4. Select ***Create Configuration Restore File*** from the Device Menu.
5. Specify the file name (must be NE2ASystem.dat) and folder in which to save the configuration restore file in the Create Configuration Restore File Dialog Box, and then click the **Save** Button.

   A dialog box for entering the device password will be displayed.



6. Set the device password, and then click the **OK** Button. A device password must be entered depending on the settings in the Restore Operation Setting Field and Run/Idle Operation Setting Field.

   The configuration restore file will be created in the specified folder.
7. Record the eight-digit ID displayed on the Network Configurator. Record the file identification ID to identify the configuration restore files in the NE2A-series Controller.



Note As soon as you create the configuration restore file, save the network configurator project to enable verifying the parameters in the configuration restore file.

Storing the Configuration Restore File on a Memory Card

Copy the configuration restore file to the root path of the Memory Card to use it with the NE2A-series Controller.

17-9-2 Validating the Configuration Restore File

With the NE2A-series Controller, it is necessary to validate the configuration restore file to change the status of the system by using a Memory Card. Unless this operation is performed, it will not be possible to use the RUN/STOP/RESTART switch or the configuration restore function.

Procedure

1,2,3...

1. Insert the Memory Card that contains the copied configuration restore file into the NE2A-series CPU Unit.
2. Confirm that the file ID to be targeted for operation is displayed on the seven-segment display of the NE2A-series Controller.
3. If the file ID is the one intended, press the SERVICE switch for at least 1 s and then release it. This will make the MC VALID indicator on the NE2A-series Controller light yellow to confirm that the configuration restore file is valid.

Once validated, the configuration restore file will remain valid until the Memory Card is removed. (It will remain valid even if the power supply of the NE2A-series Controller is turned OFF.)

17-9-3 Downloading Parameters and Locking the Configuration

Downloading Parameters

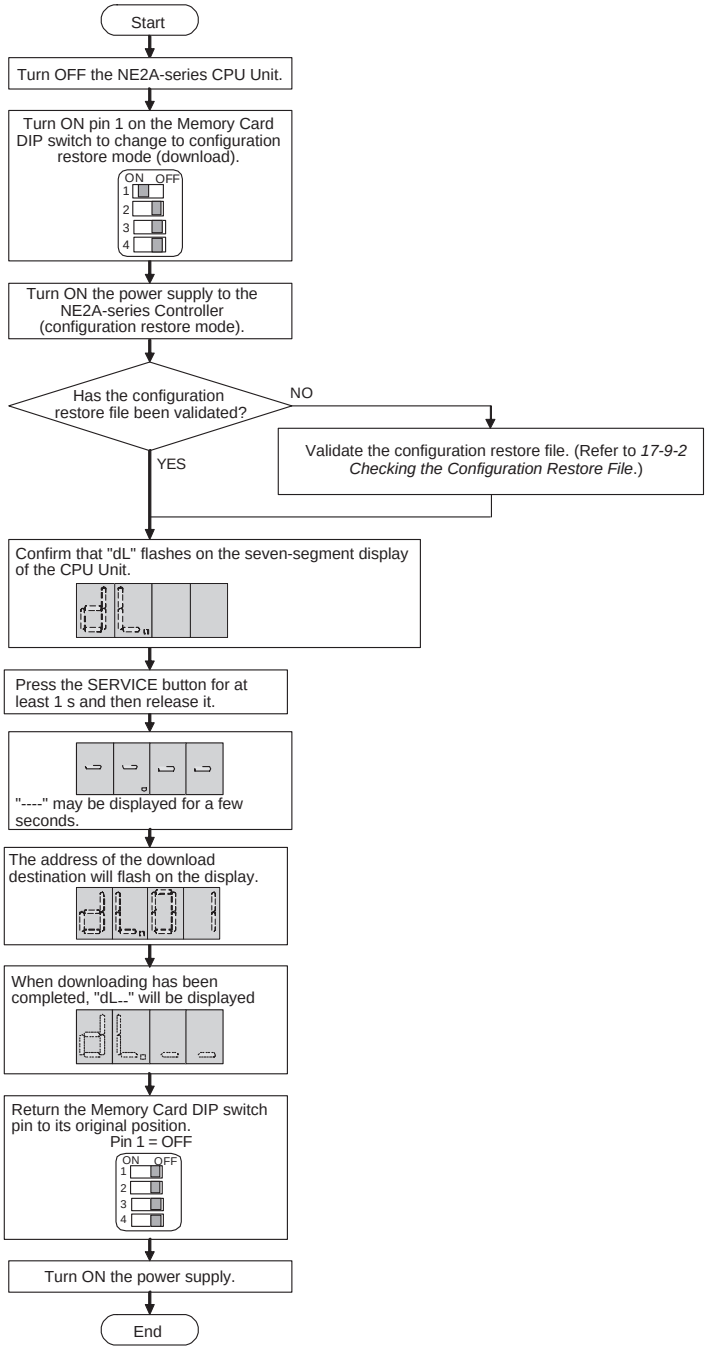
The following device parameters can be set by using a Memory Card that contains the configuration restore file.

- Parameters for the NE2A-series Controller with the Memory Card inserted and devices with connections set with the relevant NE2A-series Controller (only connections in which the relevant NE2A-series Controller is the Master)
- Parameters for the NE2A-series Controller with the Memory Card inserted and the safety devices on the same DeviceNet network

Procedure

1,2,3...

1. Turn OFF the power supply to the NE2A-series Controller.
2. Insert a Memory Card that contains the configuration restore file into the memory card slot.
3. Turn ON pin 1 (MC DOWNLOAD) on the Memory Card DIP switch.
4. Turn ON the power supply to the NE2A-series CPU Unit.
5. Confirm that the initial settings of the NE2A-series Controller have been completed.
6. Validate the configuration restore file on the seven-segment display.
7. Press the SERVICE switch on the NE2A-series Controller to execute the download.



Locking the Configuration

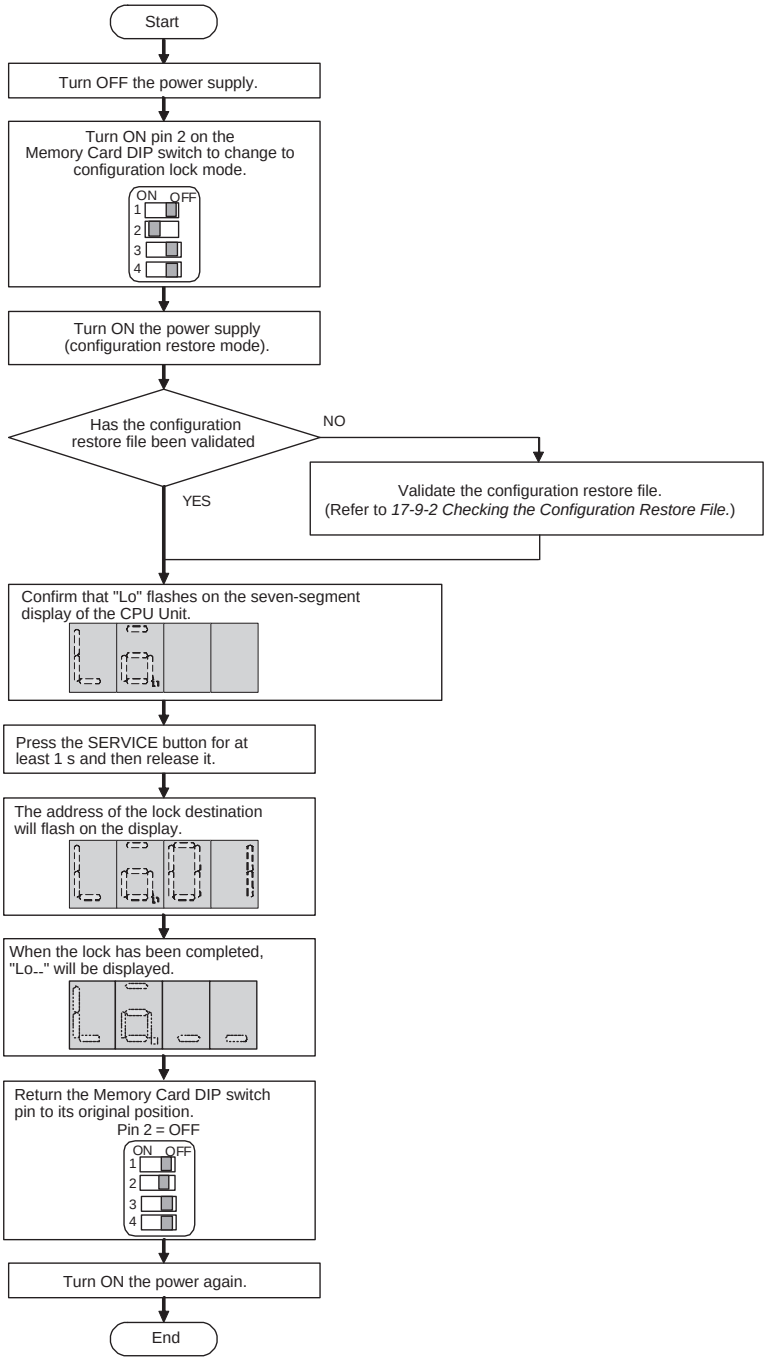
The following device configurations can be locked by using a Memory Card that contains the configuration restore file.

- Configurations for the NE2A-series Controller with the Memory Card inserted and devices with connections set with the relevant NE2A-series Controller (only connections in which the relevant NE2A-series Controller is the Master)
- Configurations for the NE2A-series Controller with the Memory Card inserted and safety devices on the same DeviceNet network

Procedure

1,2,3...

1. Turn OFF the power supply to the NE2A-series Controller.
2. Insert a Memory File that contains the configuration restore file into the memory card slot.
3. Turn ON pin 2 (MC LOCK) on the Memory Card DIP switch.
4. Turn ON the power supply to the NE2A-series CPU Unit.
5. Confirm that the initial settings of the NE2A-series Controller have been completed.
6. Validate the configuration restore file on the seven-segment display.
7. Press the SERVICE switch on the NE2A-series Controller to lock the configuration.



17-9-4 Changing the Operating Mode

Programs can be executed and stopped and operation can be restarted by using the RUN/STOP/RESTART switch on the NE2A-series CPU Unit. To use this switch, a Memory Card containing the configuration restore file must be inserted into the NE2A-series CPU Unit, and the configuration restore file must be validated.

The applicable range when starting and stopping program execution can be set to one of the following ranges in the system setup.

- Only the NE2A-series Controller with the Memory Card (Note: The operating mode of devices with set connections will not be changed.)
- The NE2A-series Controller with the Memory Card and NE1A/NE0A-series Controllers on the same DeviceNet network

Starting and Stopping Program Execution and Restarting Operation for only One NE2A-series Controller

If the following conditions are satisfied, the RUN/STOP/RESTART switch can be used to start and stop program execution and restart operation for an NE2A-series Controller.

- The target for starting and stopping program execution using the RUN/STOP/RESTART switch is set to the only the NE2A-series Controller (*Target only this device*) in the NE2A-series Controller system setup.
- The configuration restore file contains the configuration data for the NE2A-series Controller targeted for operation.
- The configuration file is inserted into the relevant NE2A-series CPU Unit, and the configuration restore file has been validated.

Starting and Stopping Program Execution for the NE1A/NE0A-series Controllers on a DeviceNet Network

The RUN/STOP/RESTART switch can be used to start and stop program execution for the other NE1A/NE0A-series Controllers on the DeviceNet network in addition to the NE2A-series Controller on which the RUN/STOP/RESTART switch is manipulated.

- The target for starting and stopping program execution or restarting operation using the RUN/STOP/RESTART switch is set to the devices connected to the network (*Target all devices on the network*) in the NE2A-series Controller system setup.
- The configuration restore file contains the configuration data for the NE1A/NE0A-series Controller.
- The Memory Card containing the configuration restore file is inserted into the NE2A-series CPU Unit, and the configuration restore file has been validated.

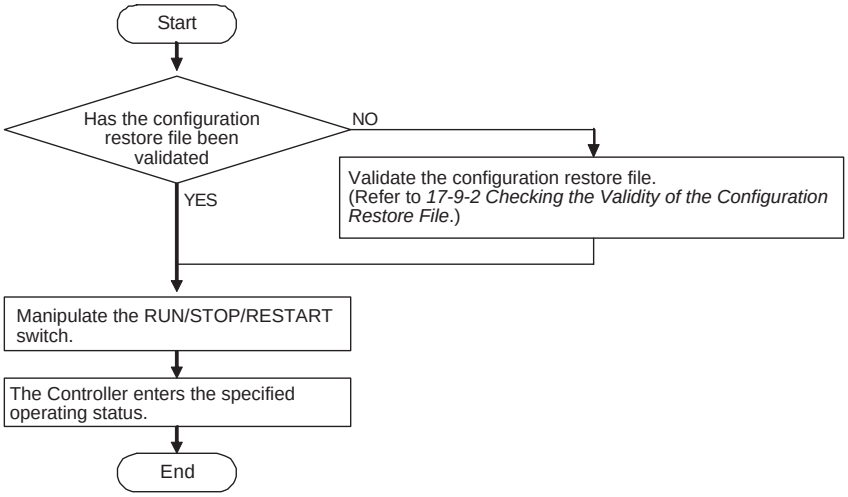
Note Only the NE2A-series Controllers that are connected to the CPU Unit in which the switch is manipulated can be restarted. The *Target all devices on the network* option does not apply when restarting.

Procedure

1,2,3...

1. Validate the configuration restore file. (Refer to *17-9-2 Checking Validity of the Configuration Restore File*.)
2. Use the RUN/STOP/RESTART switch on the NE2A-series CPU Unit to execute the run, stop, or restart operation.

Note Changing the Memory Card DIP switch is not required to change the operating mode.



Changing Operating Modes Using the RUN/STOP/START Switch or the Network Configurator

There is no particular order of priority for starting and stopping program execution by using the RUN/STOP/RESTART switch or changing the operating mode by using the Network Configurator. Therefore, use the RUN indicator to check whether execution of the program in the NE2A-series Controller is started or stopped. (Check the operating status using the MS indicator.)

SECTION 18
Checking the System Operating Status

This section describes how to check the current operating status of a NE2A-series Safety Network Controller system.

18-1 Monitoring Programs and Force-setting/resetting Variables. 464
18-1-1 Monitoring Programs 464
18-1-2 Watching Variables 464
18-1-3 Force-setting/resetting Variables 466
18-2 Monitoring Device Status in Maintenance Mode 470
18-2-1 Displaying Safety Device Status. 470
18-2-2 Monitoring Device Status 471
18-2-3 Overall Status and Error Status Monitor 473
18-2-4 Monitoring Safety Connections 474
18-2-5 Monitoring the Error History 475
18-2-6 Monitoring Local I/O Status 477
18-2-7 Monitoring the Operation Log 478
18-2-8 Manufacturing Information Monitor 479
18-3 Monitoring DeviceNet Units. 480
18-3-1 Monitoring DeviceNet Units 480
18-3-2 Unit Status Tab Page. 482
18-3-3 Communications Cycle Time Tab Page 484
18-3-4 Error History Tab Page 484
18-4 Monitoring EtherNet/IP Units. 486
18-4-1 Status Tab Page. 486
18-4-2 Error History Tab Page 487
18-4-3 Ethernet Information Tab Page 489

18-1 Monitoring Programs and Force-setting/resetting Variables

18-1-1 Monitoring Programs

The values of variables and the signal status of connections to function blocks can be monitored online in the Logic Editor Window.

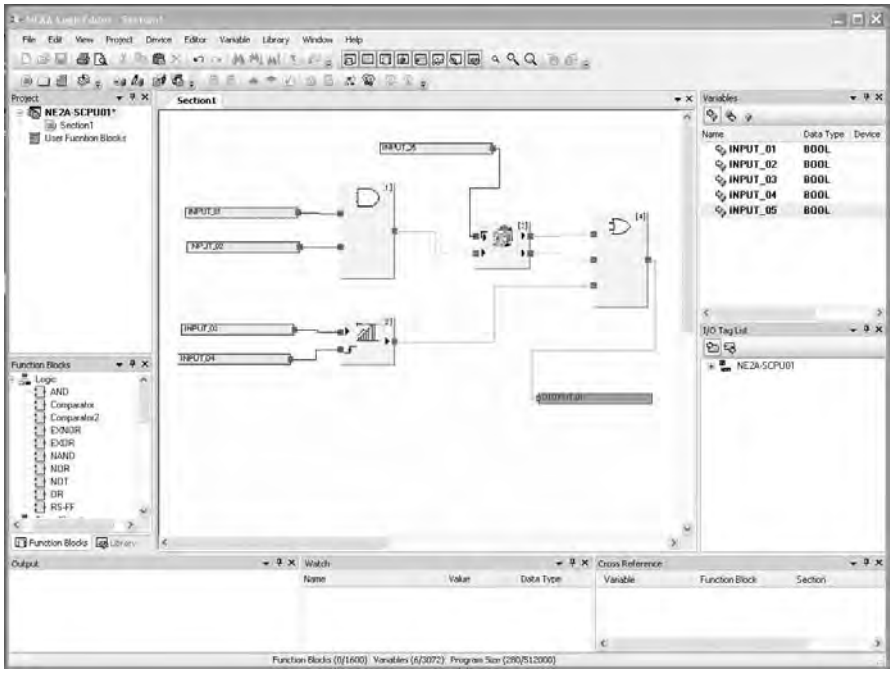
Before monitoring a program online, make sure that the Network Configurator is connected to the network, and that the NE2A-series Controller to be monitored is operating.

Starting Online Monitoring

Online monitoring will start when you select ***Monitor*** from the Device Menu.

You can also click the **Monitor** Icon ( ) in the toolbar.

A variable or connection that is currently ON will be displayed in dark green during monitoring.



Stopping Online Monitoring

To stop monitoring, select ***Monitor*** from the Device Menu while online monitoring is being performed.

You can also click the **Monitor** Icon ( ) in the toolbar.

Variables and connections are displayed in light green or black when monitoring is not being performed.

18-1-2 Watching Variables

In an NE2A-series Controller, the values of multiple variables within a program can be monitored at the same time using the Watch Window of the Logic Editor.

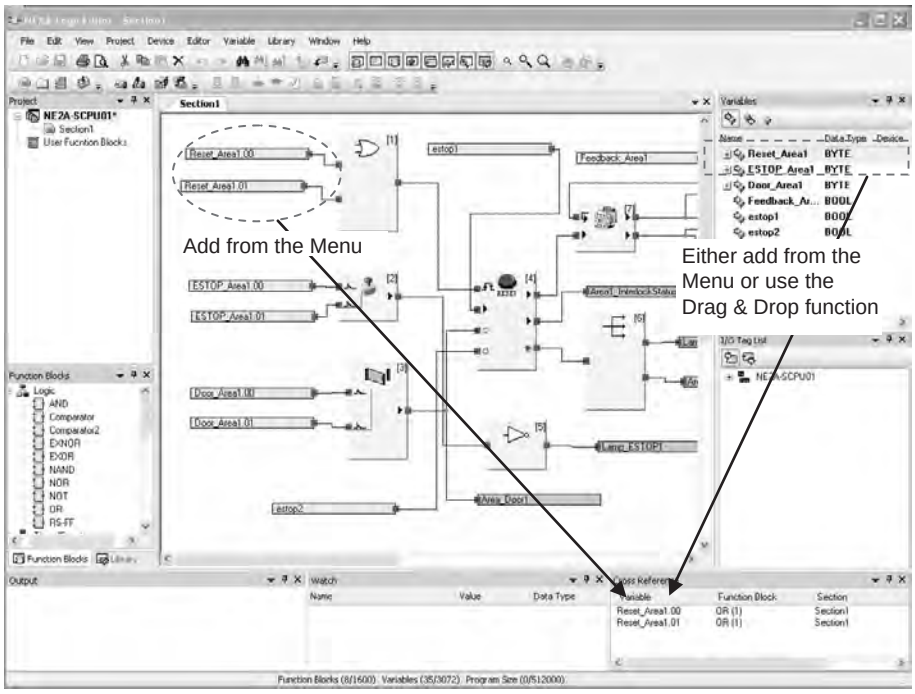
When the NE2A-series Controller is in Force Mode, variables can be force-set/reset from this window.

Registering Variables

1,2,3...

1. Select a variable either from the Variable Window or from the Program Window.
2. Select ***Add to Watch Window*** from the Variable Menu.
   You can also right-click a variable in the Variable Window or Program Window and select ***Add to Watch Window*** from the pop-up menu.

   Or, you can drag and drop a variable from the Variable Window to the Watch Window.



Deleting Registered Variables

1,2,3...

1. In the Watch Window, select the variable you want to delete.
2. Select ***Delete*** from the Edit Menu.
   You can also right-click the variable you want to delete and select ***Delete*** from the pop-up menu.

Moving Registered Variables

1,2,3...

1. In the Watch Window, select the variable you want to move.
2. Select ***Move Downward*** from the Edit Menu.
   You can also right-click the variable you want to move and select ***Move Downward*** from the pop-up menu.
   (To move a variable up, select ***Move Upward***.)

Sorting Registered Variables

Variables can be sorted by clicking on the column headings (*Name*, *Value*, or *Data type*) in the Watch Window. Sorting will alternate between descending order and ascending order each time a column heading is clicked.

Force-setting/resetting from the Watch Window

Refer to *18-1-3 Force-setting/resetting Variables*, for details.

18-1-3 Force-setting/resetting Variables

Variables that have been allocated local I/O or remote I/O can be force-set or force-reset in the Monitoring Window of the safety program. When force-setting/resetting a variable, the value of the variable used in the program can be turned ON or OFF regardless of the actual ON/OFF status of the local or remote I/O data.

Note Variables can be force-set/reset only when the configuration data of the NE2A-series Controller is unlocked.

⚠ WARNING

When data of a physical output are changed by forcing (directly or indirectly), consider possible effects before performing it. The outputs may operate, occasionally resulting in serious injury.



Force Mode

It is necessary to change the NE2A-series Controller to Force Mode to force-set/reset variables. Refer to *4-1-4 Force-setting and Force-resetting Variables*. Force-setting/resetting Variables, for details on Force Mode.

Starting Force Mode

You must input the device password to start Force Mode.

Also, you can start Force Mode only when the configuration data of the NE2A-series Controller is unlocked.

Monitoring Force Mode Time

A limit can be set for the time that the NE2A-series Controller will continue in Force Mode. The duration time is specified when Force Mode is started or restarted. The upper limit of the time is 24 hours.

The NE2A-series Controller will end Force Mode and enter IDLE Mode in Normal Mode when the specified duration time elapses.

Note Take sufficient safety measures because variables that have been force-set or force-reset will change to reflect the actual I/O status when the specified time elapses.

Ending Force Mode

You can end Force Mode in the following three ways:

Ending Force Mode with the Network Configurator

- The NE2A-series Controller moves to IDLE Mode in Normal Mode when Force Mode is ended.

Elapse of Force Mode Duration Time

The NE2A-series Controller will enter IDLE Mode in Normal Mode when the specified duration time elapses if the Force Mode time is monitored.

Changing the NE2A-series Controller to a Mode Other Than IDLE or RUN Mode

When you perform a download or reset operation, turn OFF the power supply, or change the node address switches, the NE2A-series Controller will move to the CONFIGURING Mode and the Force Mode will be cancelled.

The Force Mode will continue, however, if a change is made between IDLE Mode and RUN Mode.

Force Mode at Startup

If the power supply is turned OFF while the NE2A-series Controller is in Force Mode, the Controller will start the next time in Normal Mode. Start the Force Mode again, if required.

Procedure and Windows

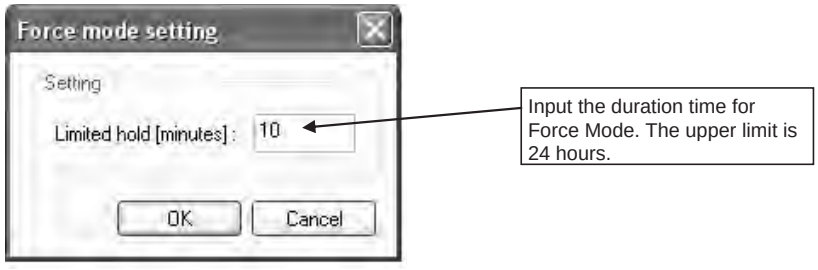
■ Starting Force Mode

Use the following procedure in the monitoring window of the Logic Editor to start the Force Mode and enable force set or force reset operations.

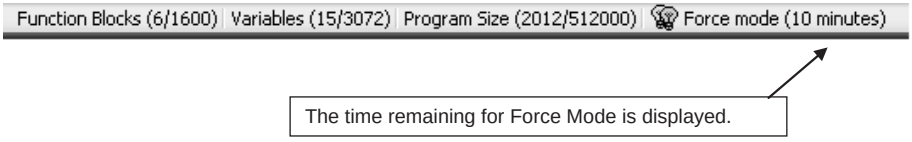
1,2,3... 1. Select ***Force Mode - Enable*** from the Device Menu. You can also click the **Force Mode** Icon on in the toolbar.



The Force Mode Setting Dialog Box will be displayed.



2. Set the time for executing Force Mode, and then click the **OK** Button. When the dialog box for entering the device password is displayed, enter the device password, and then click the **OK** Button. The system will enter Force Mode.
   - Force Mode will be displayed on toolbar.
   - The status of the Force Mode icon on toolbar will change.



■ Ending Force Mode

Use the following procedure in the monitor window of the Logic Editor to end Force Mode.

Select ***Force Mode - Disable*** from the Device Menu.

You can also click the **Force Mode** Icon in the toolbar.

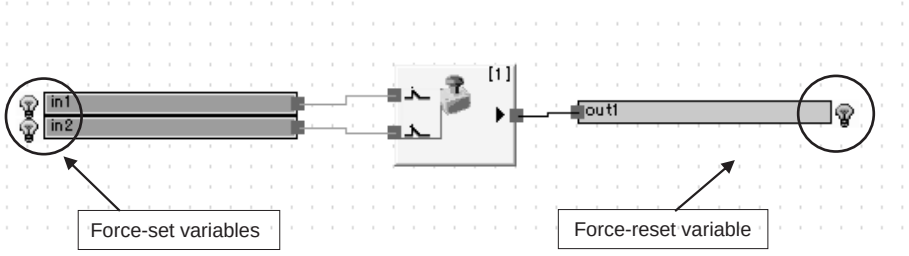


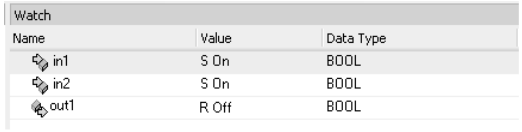
■ Force-setting and Force-resetting Variables

In the monitor Window, select the variable to be force-set or force-reset.

Operation	Command procedure	Toolbar	Description
Force-setting a variable	***Device - Force Mode - Force ON***		The output will be turned ON regardless of the actual ON/OFF status.
Force-resetting a variable	***Device - Force Mode - Force OFF***		The output will be turned OFF regardless of the actual ON/OFF status.
Cancel individual forced status	***Device - Force Mode - Force Release***	---	The force-set status or force-reset status will be cleared and the variable will return to the actual ON/OFF status.
Canceling all forced status	***Device - Force Mode - Force Release All***	---	The force-set status or force-reset status will be cleared for all variables and the variables will return to the actual ON/OFF status.
Displaying forced status	***Device - Force Mode - Upload Forced List***	---	The force-set variables or force-reset variables will be added to the Watch Window.

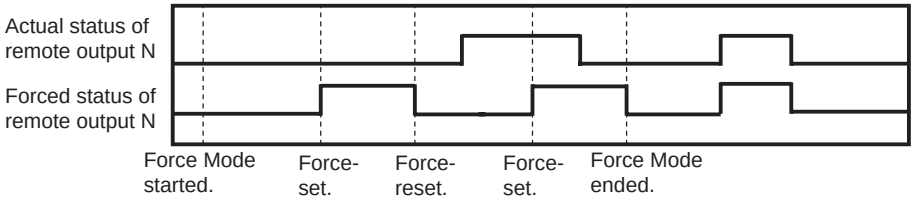
You can also right-click the variable in the Watch Window and select the variable to be force-set or force-reset from the list that is displayed.





S: Force-set variables
R: Force-reset variables

The variables that were force-set or force-reset will return to the actual I/O values when Force Mode of the NE2A-series Controller is ended.



Note When the force-set/force-reset status of a variable is cleared, the variable will turn OFF and then be updated with the latest status in the next cycle.

Continuing in Force Mode When Exiting the Network Configurator

It is possible to close the Logic Editor and exit the Network Configurator and continue in the Force Mode. The NE2A-series Controller will retain the force-setting/resetting status until the set time has elapsed.

Exiting the Network Configurator

When the Logic Editor is closed and the Network Configurator is exited, the force-setting or force-resetting status set until that point will be held.

Restarting Procedure

Once the Logic Editor has been closed, the rights to perform force-setting and force-resetting will be lost. To perform force-setting or force-resetting again, select ***Force Mode - Start*** from the Device Menu, and then enter the device password and continuation time.

It is possible to obtain rights to perform force-setting and force-resetting while retaining the force-setting and force-resetting status for presently set variables.

Force-setting and Force-resetting from Multiple Logic Editors

Force-setting and force-resetting can be performed for an NE2A-series Controller only from the Logic Editor that was last to perform the force-start procedure.

If force-setting or force-resetting is being executed on one Logic Editor (1st) and the force-start operation is performed from another Logic Editor (2nd), it will be possible to perform force-setting and force-resetting operations only from the 2nd Logic Editor. It will no longer be possible to perform force-setting and force-resetting operations from the 1st Logic Editor.

Extending the Force Mode Continuation Time

To extend the Force Mode continuation time, close the Logic Editor and then start it again. The continuation time can be set again with the Force Mode starting procedure.

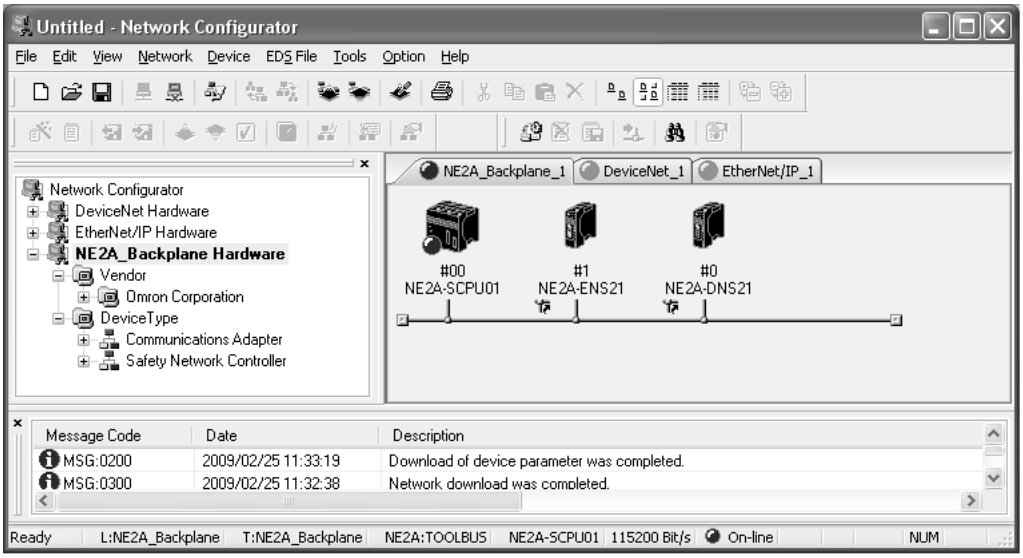
18-2 Monitoring Device Status in Maintenance Mode

The status information or history information on an NE2A-series Controller can be monitored online using the Network Configurator.

18-2-1 Displaying Safety Device Status

Displaying Device Status

Status information on the Safety Devices for an NE2A-series Controller can be displayed on the Maintenance Mode display. An example is shown below.



Moving to Maintenance Mode

The icons displayed at this time indicate the following status.

Icon	Status
Gray with white border	Online status
Gray with green border	Default status (not configured)
Green	Idle status
Blue	Normal execution status
Yellow	Warning status
Red	Alarm status

Refer to *9-6-2 Network Configuration Pane*, for details on the status.

Refreshing the Device Status Display

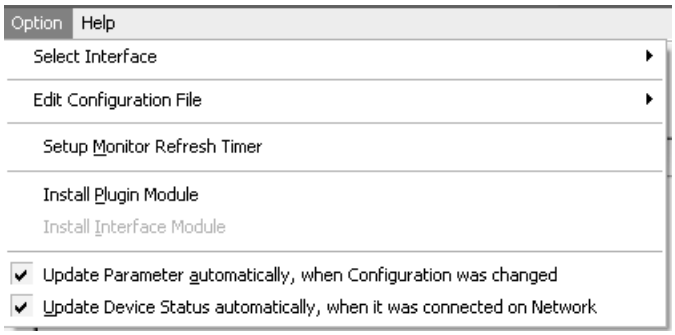
The display of device status is refreshed automatically if any of the following operations is executed in the Network Configurator.

- Uploading the network
- Downloading the network
- Downloading parameters
- Updating maintenance information
- Changing the device mode (RUN/IDLE)
- Resetting a device

The display can also be refreshed at any time while connected online by selecting ***Update Device Status*** from the Network Menu.

Automatic Refreshing of Device Status Display

When the Network Configurator is connected to the system and is connected online, device information is received automatically and can be displayed. To have the device status refreshed and displayed immediately upon connecting online, select ***Update Device Status automatically, when it was connected on Network*** from the Options Menu.



18-2-2 Monitoring Device Status

The status of the NE2A, NE1A, NE0A, and DST1 can be monitored from the Network Configurator. Detailed information on any errors occurring in the device can also be monitored.

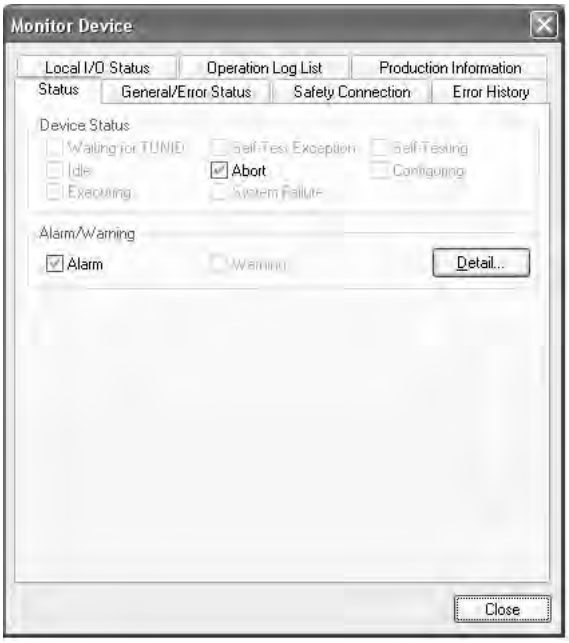
Refer to the manual for each Controller for information on monitoring status for the NE1A, NE0A, or DST1.

Monitoring Status from the Network Configurator

Procedure

1,2,3...

1. Select the device whose status is to be monitored.
2. Select ***Monitor*** from the Device Menu.
   You can also right-click the device and select ***Monitor*** from the pop-up menu.
   Or, you can click the **Monitor Device** Icon ( ) in the toolbar.
   The Monitor Device Dialog Box will be displayed.
3. Click the **Status** Tab.
   The Status Tab Page will be displayed.



Device Status Area

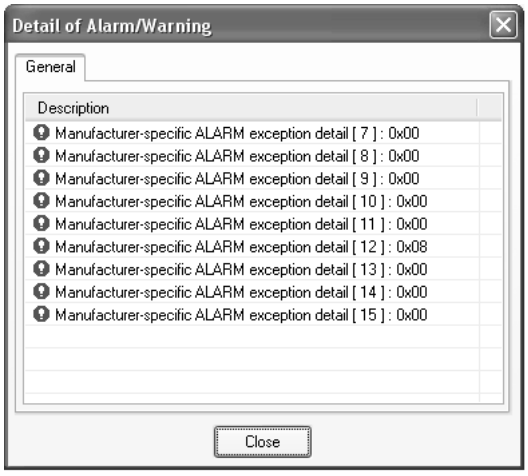
The device status area displays the status of the device.
The device can be in any of the following status.

Device status	Description
Waiting for TUNID setting	Waiting for the configuration data to be downloaded.
Idling	Initialization is complete and the Controller is waiting to move to RUN Mode. This is called IDLE Mode.
Running	All functions, including the Safety Logic, are running. This is called RUN Mode.
Self-test error	An error occurred during self-testing.
Abort	A minor error has occurred.
System Failure	A critical error has occurred.
Self-testing	Self-diagnosis is being performed to ensure safety functions.
Configuring	Downloading the configuration data.

Alarm/Warning Area

The Alarm/Warning Area shows errors that have occurred in the device.

Click the **Detail** Button to see information on the error that has occurred. An alarm is indicated with the Icon. A warning is indicated with the Icon.



The Detail of Alarm/Warning Dialog Box contains the General, Safety Output, Safety Input, and Test Output Tab Pages. The General Tab Page displays the errors that have occurred in the Unit. The other tab pages display the errors that have occurred in the input terminals, output terminals, and test output terminals.

Devices will not operate normally if an alarm occurs. You must remove the cause of the alarm. Devices will continue to operate when a warning occurs, but it is recommended that the cause of the warning be removed because problems may occur later.

18-2-3 Overall Status and Error Status Monitor

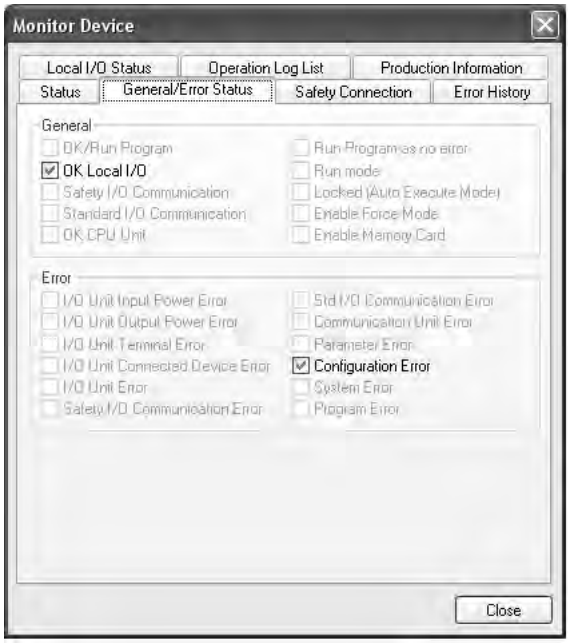
The status details and error details for an NE2A-series Controller can be monitored from the Network Configurator. This will enable you to identify which Unit has an error and check if an error has occurred in the Safety Connections or Standard Communications.

The connection information of a DST1-series Controller cannot be monitored.

Monitoring from the Network Configurator

1,2,3...

1. Select the device whose status is to be monitored.
2. Select ***Monitor*** from the Device Menu.
   You can also right-click the device and select ***Monitor*** from the pop-up menu.
   Or, you can click the **Monitor Device** Icon ( ) in the toolbar.
   The Monitor Device Dialog Box will be displayed.
3. Click the **General/Error Status** Tab.
   The General/Error Status Tab Page will be displayed.



Overall Unit Status

For details on each item, refer to *Overall Unit Status* on page 124.

Error Status

For details on each item, refer to *Error Status* on page 125.

18-2-4 Monitoring Safety Connections

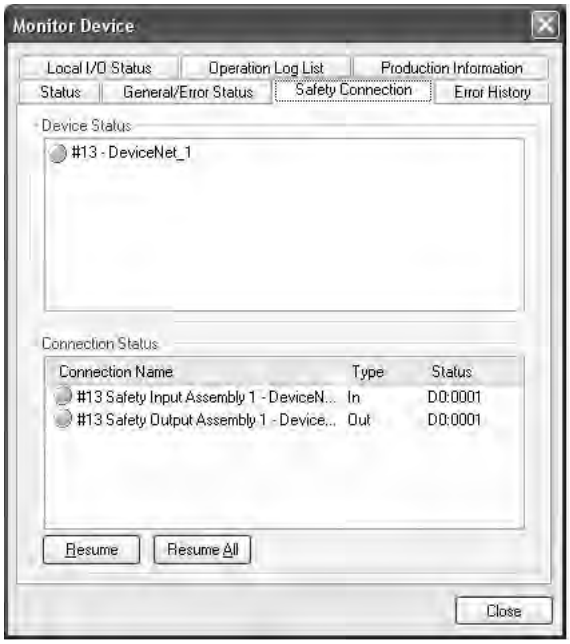
The status of Safety Connections for an NE2A-series Controller can be monitored from the Network Configurator. This will enable you to identify devices with which safety communications could not be established properly, or the Safety Connections for which an error has occurred.

The connection information of a DST1-series Controller cannot be monitored.

Monitoring from the Network Configurator

1,2,3...

1. Select the device whose status is to be monitored.
2. Select ***Monitor*** from the Device Menu.
   You can also right-click the device and select ***Monitor*** from the pop-up menu.
   Or, you can click the **Monitor Device** Icon ( ) in the toolbar.
   The Monitor Device Dialog Box will be displayed.
3. Click the **Status** Tab.
   The Status Tab Page will be displayed.



The status codes (i.e., error codes) can be monitored. By monitoring the status codes when a failure occurs in establishing a connection, the cause of the failure can be checked based on the status code returned from the Target device. Refer to *SECTION 19 Troubleshooting* for details on the status codes.

Also, if Connection Stop Mode is selected for communications errors, you can use this dialog box to restart the connection. In this dialog box, if you click the **Resume** Button after selecting the stopped connection from the Connection Status, communications to the specified connection can be established again.

If you click the **Resume All** Button, I/O communications can be established again for all Slaves for which I/O communications have stopped. Repeated attempts will be made until all connections are resumed.

18-2-5 Monitoring the Error History

The error history of the NE2A, NE1A, NE0A, or DST1 can be monitored from the Network Configurator.

An NE2A-series Controller can internally store up to 100 records in the error history. If any more errors occur, the oldest records will be deleted.

The errors that are stored in the error history include errors that are saved in the non-volatile memory and are not deleted even when the power is turned OFF, and error that are saved in the RAM and are deleted when the power is turned OFF.

For details on errors of the NE2A-series Controller, refer to *SECTION 19 Troubleshooting*.

For details on the error history monitor for NE2A-series DeviceNet Units and EtherNet Units, refer to *18-3 Monitoring DeviceNet Units* and *18-4 Monitoring EtherNet/IP Units*.

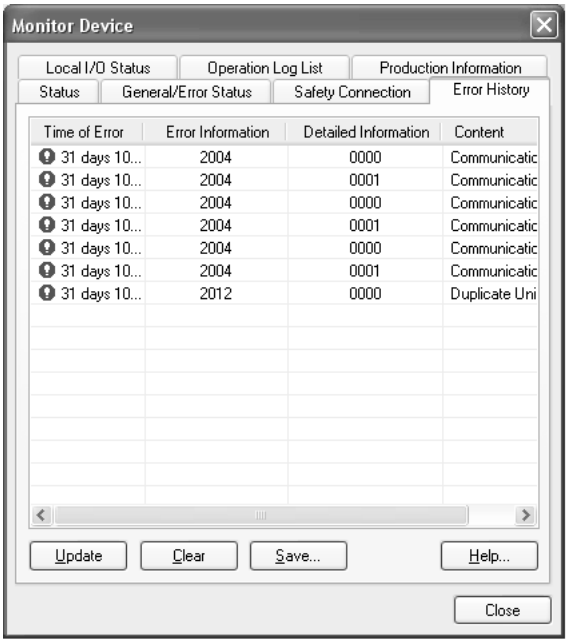
For details on NE1A, NE0A, and DST-series Controllers, refer to the user's manual of the Controller.

Monitoring from the Network Configurator

Procedure

1,2,3...

1. Select the device whose status is to be monitored.
2. Select ***Monitor*** from the Device Menu.
   You can also right-click the device and select ***Monitor*** from the pop-up menu.
   Or, you can click the **Monitor Device** Icon ( ) in the toolbar.
   The Monitor Device Dialog Box will be displayed.
3. Click the **Error History** Tab.
   The Error History Tab Page will be displayed.



The displayed items are described in the following table.

Item	Description
Time of Error	Displays the conduction time of the device when an error occurs. However, 0 is displayed at all times for a DST1-series Controller.
Error Information	Displays the error code.
Detailed Information	Displays detailed information on the error code.
Content	Describes the error.

Updating the Error History

Click the **Update** Button to monitor the most recent error history.

Clearing the Error History

Click the **Clear** Button to delete the error history saved internally in the NE2A, NE1A, NE0A, or DST1.

Saving the Error History

The error history information can be saved in the CSV format. Click the **Save** Button to save the error history.

18-2-6 Monitoring Local I/O Status

You can monitor the contact operation counter of the Safety Input Status, Test Output Status, and Safety Output Status.

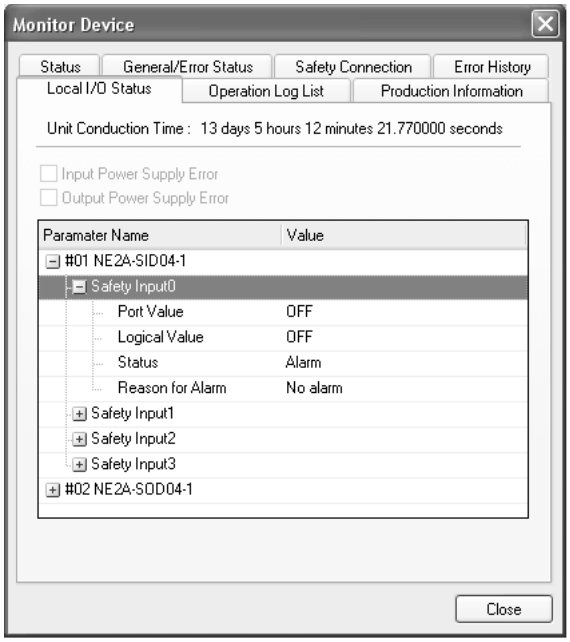
Monitoring from the Network Configurator

The local I/O status can be monitored by using the following procedure.

Procedure

1,2,3...

1. Select the device whose status is to be monitored.
2. Select either ***Monitor*** or ***Maintenance Information*** from the Device Menu.
   You can also right-click the device and select ***Monitor*** or ***Maintenance Information*** from the pop-up menu.
   Or, you can click the **Monitor Device** Icon ( ) or **Maintenance Information** Icon ( ) in the toolbar.
   The Monitor Device Dialog Box will be displayed.
3. Click the **Local I/O Status** Tab.
   The Local I/O Status Tab Page will be displayed.



The displayed items are described in the following table.

Item	Description
Unit Conduction Time	Displays the conduction time after the power supply to the Unit is turned ON.
Input Power Supply Error	Selected if an input power supply error has occurred.
Output Power Supply Error	Selected if an output power supply error has occurred.

Item	Description	
Parameter Name	**I/O port value**	Value before evaluation for safety I/O
	I/O logic value	Value after evaluation for safety I/O
	Status	OK: Normal, NG: Error
	Cause of error	Refer to*19) I/O Unit Error Status* on page 134.

18-2-7 Monitoring the Operation Log

The NE2A-series Controller saves a log of the operations performed for the Controller. This log can be monitored, cleared, and saved in the computer with the help of the Logic Editor.

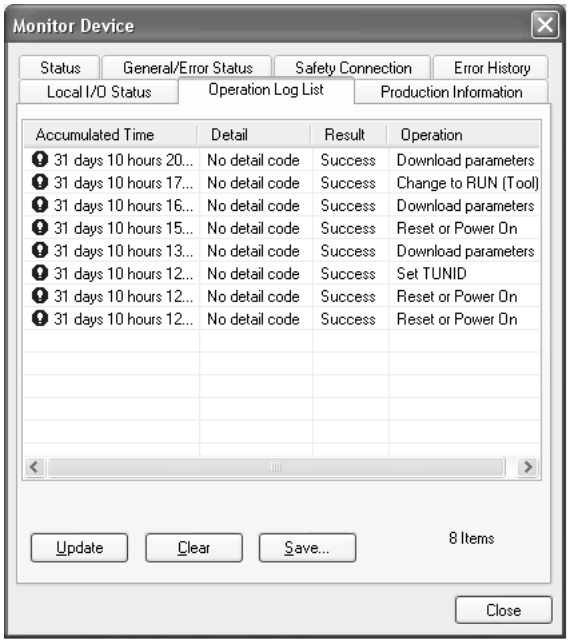
Monitoring from the Network Configurator

Procedure

1,2,3... 1. Select the device whose status is to be monitored.

2. Select **Monitor** from the Device Menu.
   You can also right-click the device and select ***Monitor*** from the pop-up menu.
   Or, you can click the **Monitor Device** Icon ( ) in the toolbar.
   The Monitor Device Dialog Box will be displayed.

3. Click the **Operation Log List** Tab.
   The Operation Log List Tab Page will be displayed.



The displayed items are described in the following table.

Item	Description
Accumulated Time (Microseconds)	Displays the cumulative time when the operation was executed.
Detail	Displays detailed information on the operation.
Operation	Displays the operation that was saved.
Result	Displays the result of the operation.

Updating the Operation Log

Click the **Update** Button to monitor the most recent operation log.

Clearing the Operation Log

Click the **Clear** Button to delete the operation log saved internally in the NE2A, NE1A, NE0A, or DST1.

Exporting the Operation Log

The operation log information can be saved in the CSV format. Click the **Export** Button to save the information.

Operations That Are Saved

A log of the following operations is saved.

NE2A-series Controllers

- Turning ON the power supply
- Changing to RUN Mode
- Changing to STOP Mode
- Resetting
- Restoring memory with a Memory Card
- Locking with the Memory Card

Network Configurator

- Setting a TUNID
- Downloading parameters
- Locking
- Unlocking
- Changing to RUN Mode
- Changing to STOP Mode
- Starting Force Mode
- Ending Force Mode
- Force Mode timeout
- Resetting
- Changing the device password (initialization)
- Clearing the error history

Note The entire operation log will be deleted when you reset to the default settings with the Network Configurator or Logic Editor.

18-2-8 Manufacturing Information Monitor

The manufacturing information on the NE2A CPU Unit can be displayed.

18-3 Monitoring DeviceNet Units

18-3-1 Monitoring DeviceNet Units

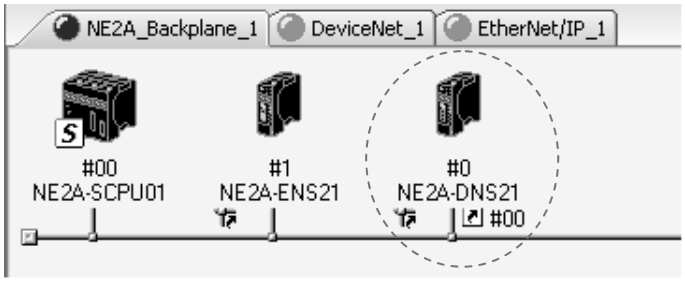
Description

You can monitor detailed information, such as the status of the DeviceNet Unit or individual devices, and also error histories.

Monitoring DeviceNet Units from the Network Configurator

Procedure

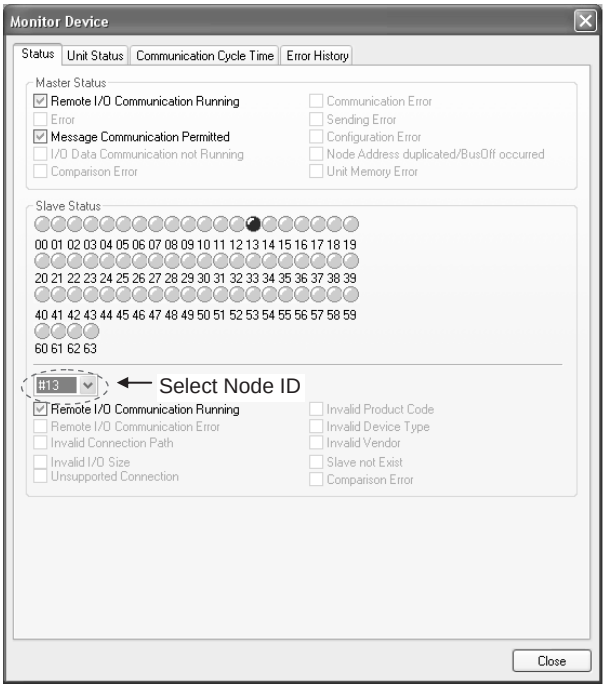
1,2,3... 1. Select the NE2A-DNS21 device whose status is to be monitored.



2. Select ***Monitor*** from the Device Menu.
   You can also right-click the device and select ***Monitor*** from the pop-up menu.
   Or, you can click the **Monitor Device** Icon ( ) in the toolbar.
   The Monitor Device Dialog Box will be displayed.
   The tab pages and details are described below.

Status Tab Page

The following tab page will be displayed when you click the **Status** Tab in the Monitor Device Dialog Box.



Master Function Status Area

The items displayed in the Master Function Status Area are described in the following table.

Item	Description
Remote I/O Communication Running	Indicates that remote I/O communications is operating for the Master.
Error	Indicates that one of the following errors has occurred: verification error, communications error, transmission error, configuration error, duplicated node address, Bus Off error, or unit memory error.
Message Communication Permitted	Indicates that the device is connected online.
I/O Data Communication not Running	This is the reverse of the Remote I/O Communication Running Check Box.
Comparison Error	Indicates that the Slave information registered in the scan list is different from the information in the Slave.
Communication Error	Indicates that a communications error occurred in the Slave I/O connection.
Sending Error	Indicates that either a network power error or a send timeout occurred.
Configuration Error	Indicates that one of the following errors occurred: • Invalid message monitoring timer list data • Invalid scan list data • Master I/O refresh error
Node Address duplicated/ Bus Off occurred	Indicates that an error was found in the node address duplication check performed at Unit startup, or that a Bus Off error (communications stopped due to heavy communications traffic) occurred. The device will remain offline and all communications will be stopped.
Unit Memory Error	Indicates that an error exists in the internal memory where the error history is saved.

Slave Function Status Area

The Slave Function Status Area provides detailed information on the Slave condition or status. The status of the Slave is indicated by the following status icons.

Status Icon	Status
(Gray icon with light blue border)	Remote I/O communications are not operating.
(Blue icon)	Remote I/O communications are operating.
(Red icon)	An error occurred.

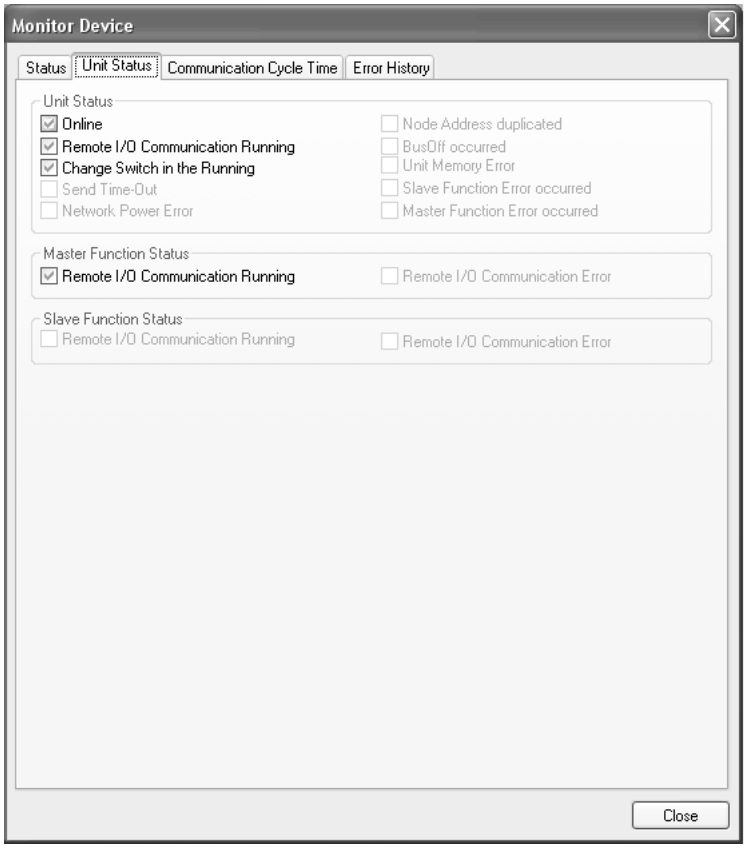
Select the Node ID of the device whose status is to be viewed from the Select Node ID Field. The Slave status of the selected device will be displayed. (The check boxes in the Slave Function Status Area will be selected to show the status of the Slave.) The items displayed in the Slave Function Status Area are described below.

Item	Description
Remote I/O Communication Running	Indicates that remote I/O communications are operating.
Remote I/O Communication Error	Indicates that a timeout has occurred in remote I/O communications with a Slave for which remote I/O communications were in progress

Item	Description
Invalid Connection Path	Indicates that an attempt to set up a connection path registered in the scan list has failed.
Invalid I/O Size	Indicates that the I/O size registered in the scan list does not match the I/O size of the Slave.
Unsupported Connection	Indicates that the Slave does not support the connection registered in the scan list.
Invalid Product Code	Indicates that the product code registered in the scan list does not match the product code of the Slave.
Invalid Device Type	Indicates that the device type registered in the scan list does not match the device type of the Slave.
Invalid Vendor	Indicates that the vendor registered in the scan list does not match the Slave vendor.
Slave not Exist	Indicates that the Slave registered in the scan list does not exist.
Comparison Error	Indicates that the Slave information registered in the scan list is different from the actual Slave information.

18-3-2 Unit Status Tab Page

The following tab page will be displayed when you click the **Unit Status** Tab in the Monitor Device Dialog Box.



Unit Status Area

The items displayed in the Unit Status Area are described below.

Item	Description
Online	Indicates that the device is connected online.
Remote I/O Communication Running	Indicates that the remote I/O communications for the Master are operating.

Item	Description
Switch Change during Operation	Indicates that the hardware switch was changed during operation.
Send Time-Out	Indicates that a timeout occurred while sending data due to one of the following reasons: • Not even one Slave exists • The baud rates are not the same.
Network Power Error	Indicates that power is not being supplied to the network.
Node Address duplicated	Indicates that an error was found in the node address duplication check performed during Unit startup.
Bus Off occurred	Indicates that a Bus Off error (communications stopped due to heavy communications traffic) occurred.
Unit Memory Error	Indicates that an error exists in the internal memory where the error history is saved.
Slave Function Error Occurred	Indicates that one or more errors have occurred in the Slave.
Master Function Error occurred	Indicates that one or more errors have occurred in the Master.

Master Function Status Area

The items displayed in the Master Function Status Area are described in the following table.

Item	Description
I/O Data Communication Running	Indicates that remote I/O communications are in progress with one or more Slaves.
Remote I/O Communication Error	Indicates that a timeout has occurred in remote I/O communications with a Slave for which remote I/O communications were in progress.

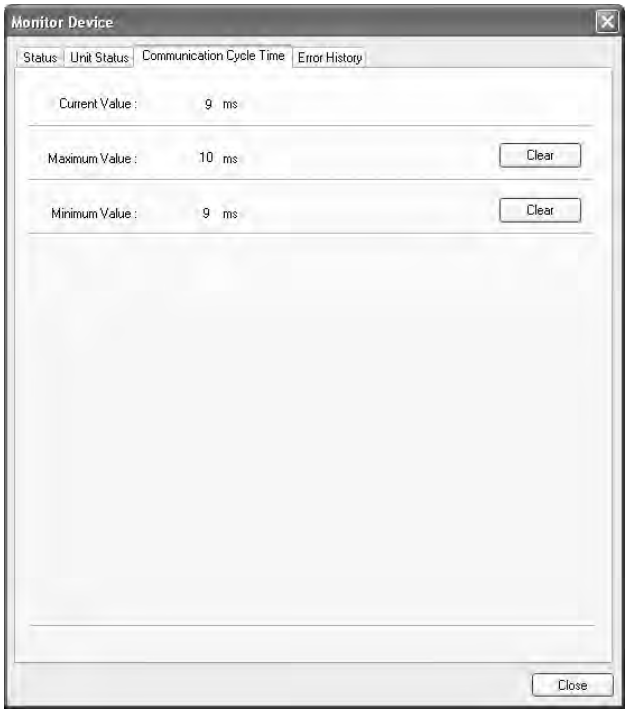
Slave Function Status Area

The items displayed in the Slave Function Status Area are described in the following table.

Item	Description
I/O Data Communication Running	Indicates that the Slave is performing remote I/O communications normally with the Master.
Remote I/O Communication Error	Indicates that a communications error occurred in the Slave I/O connection.

18-3-3 Communications Cycle Time Tab Page

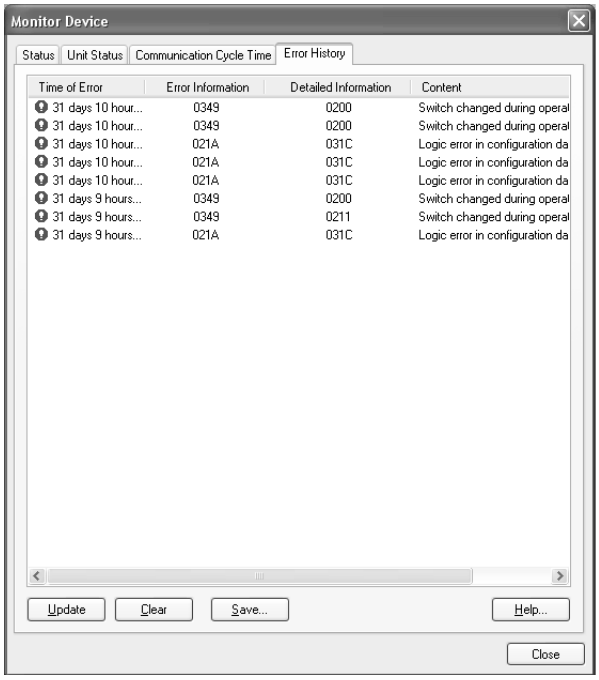
The following tab page will be displayed when you click the **Communications Cycle Time** Tab in the Monitor Device Dialog Box.



The value for the Communications Unit will be cleared when you click the **Clear** Button for the maximum value or minimum value.

18-3-4 Error History Tab Page

The following tab page will be displayed when you click the **Error History** Tab in the Monitor Device Dialog Box.



The items displayed on the tab page are described in the following table.

Item	Description
Time of Error	Displays the conduction time of the device when the error occurred.
Error Information	Displays the error code.
Detailed Information	Displays detailed information on the error code.
Content	Describes the error.

Updating the Error History

Click the **Update** Button to monitor the most recent error history.

Clearing the Error History

Click the **Clear** Button to delete the error history saved in the DeviceNet Unit.

Saving the Error History

The error history information can be saved in the CSV format. Click the **Save** Button to save the error history.

18-4 Monitoring EtherNet/IP Units

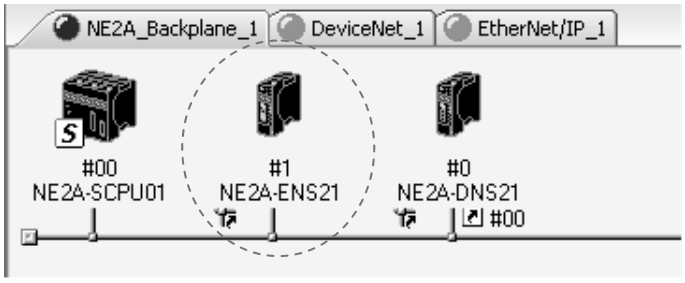
Description

You can monitor detailed information, such as the status of the EtherNet/IP Unit or devices, and also the error history.

Monitoring an EtherNet/IP Unit with the Network Configurator

Procedure

1,2,3... 1. Select the NE2A-ENS21 device whose status is to be monitored.



2. Select ***Monitor*** from the Device Menu.
   You can also right-click the device and select ***Monitor*** from the pop-up menu.
   Or, you can click the **Monitor Device** Icon ( ) in the toolbar.
   The Monitor Device Dialog Box will be displayed.
   The tab pages and details are described below.

18-4-1 Status Tab Page

The following tab page will be displayed when you click the **Status** Tab in the Monitor Device Dialog Box.



Unit Status Area

The items displayed in the Unit Status Area are described in the following table.

Item	Description
Unit Error	Indicates that an error has occurred in the operation of the EtherNet/IP Unit.
Network Error	Indicates that one or more errors have occurred in the network.
Unit Memory Error	Indicates that an error occurred while trying to access the internal nonvolatile memory of the Unit.
Com. Controller Error	Indicates that an error occurred in the communications controller.
IP Address Duplicated	Indicates that a duplication was found for the specified IP address.
LINK OFF Error	Indicates that an error occurred while trying to establish a link between switching hubs.
On-Line	Indicates that the device is online. (Internal communications processing of the EtherNet/IP unit can be executed.)
Change IP address in Run mode	Indicates that the node address setting switch was changed after the power supply was turned ON.
Error History	Indicates that there is one or more records in the error history.

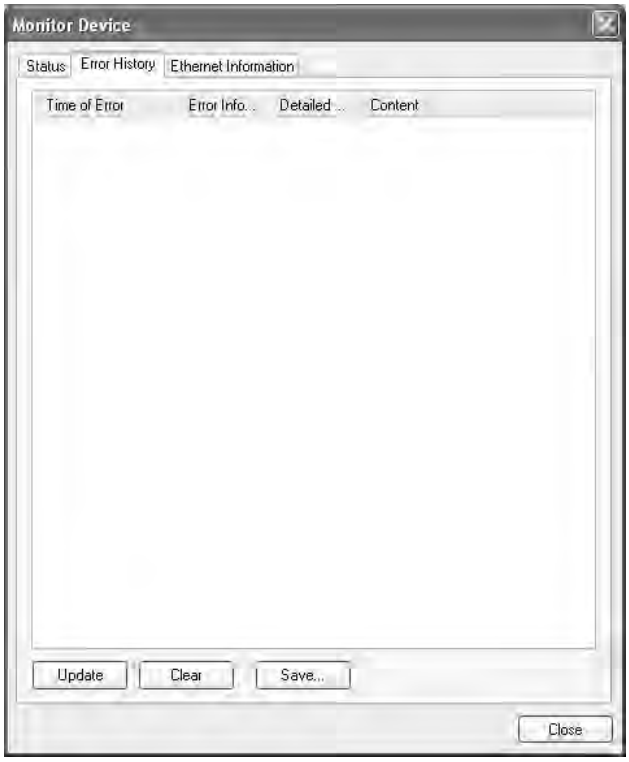
Network Status Area

The items displayed in the Network Status Area are described in the following table.

Item	Description
Invalid Parameter	Indicates that either an error was detected in the validity check of the parameters related to the Tag Data Link saved in the nonvolatile memory, or an error was found in a checksum.
Ethernet Link Status	Ethernet Link Status
Ethernet Config Logical Error	Indicates that the following parameters are invalid: • TCP/IP settings (IP address, subnet mask, link setting)
IP Address Create Logical Error	Indicates that the IP address table is invalid.
BOOTP Server Error	Indicates that one of the following errors occurred during usage of the BOOTP server • The IP address received from the server is invalid. • A timeout occurred while communicating with the server.

18-4-2 Error History Tab Page

The following tab page will be displayed when you click the **Error History** Tab in the Monitor Device Dialog Box.



The items displayed on the tab page are described in the following table.

Item	Description
Time of Error	Displays the conduction time of the device when the error occurred.
Error Information	Displays the error code.
Detailed Information	Displays detailed information on the error code.
Content	Describes the error.

Updating the Error History

Click the **Update** Button to monitor the most recent error history.

Clearing the Error History

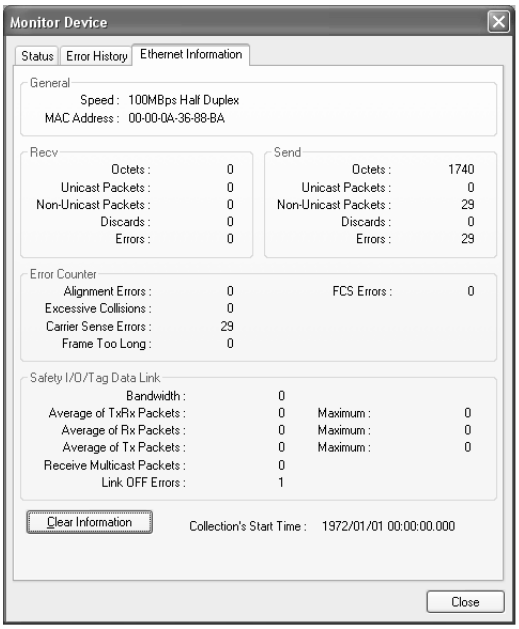
Click the **Clear** Button to delete the error history saved in the EtherNet/IP Unit.

Saving the Error History

The error history information can be saved in the CSV format. Click the **Save** Button to save the error history.

18-4-3 Ethernet Information Tab Page

The following tab page will be displayed when you click the **Ethernet Information** Tab in the Monitor Device Dialog Box.



The received and sent data that is displayed on the tab page will be cleared when you click the **Clear Send** and **Recv Info** Button.

The error counter data that is displayed in the dialog box will be cleared when you click the **Clear Error Counter** Button.

General Area

The items displayed in the General Area are described in the following table.

Item	Description
Speed	Displays the Ethernet baud rate.
MAC Address	Displays the Ethernet address of the device.

Recv Area

The items displayed in the Recv Area are described in the following table.

Item	Description
Octets	Displays the number of bytes of received data.
Unicast Packets	Displays the number of packets of data received from a specific device.
Non-Unicast Packets	Displays the number of packets of data received from other than a specific device.
Discards	Displays the number of packets of received data that has been discarded.
Errors	Displays the number of packets of received data that have resulted in an error.

Send Area

The items displayed in the Send Area are described in the following table.

Item	Description
Octets	Displays the number of bytes of sent data.
Unicast Packets	Displays the number of packets of data sent to a specific device.

Item	Description
Non-Unicast Packets	Displays the number of packets of data sent to other than a specific device.
Discards	Displays the number of packets of sent data to be discarded.
Errors	Displays the number of packets of sent data that have resulted in an error.

Error Counter Area

The items displayed in the Error Counter Area are described in the following table.

Item	Description
Alignment Errors	Displays the number of received frames whose length cannot be expressed as an octet integer.
Excessive Collisions	Displays the number of times send errors occurred due to collisions.
Carrier Sense Errors	Displays the number of times the carrier sense condition was lost or assertion was not performed during an attempt to send a frame.
Frame Too Long	Displays the number of times errors occurred in the data length.
FCS Errors	Displays the number of times an FCS error occurred in a packet.

Safety I/O/Tag Data Link Area

This area displays the status of the tag data links.

Clear Information Button

Click this button to clear the information from the Recv, Send, Error Counter, and Safety I/O/Tag Data Link Areas.

Collection's Start Time

The time is always "1972/01/01 00:00:00:000" with an NE2A-series EtherNet/IP Unit.

SECTION 19
Troubleshooting

This section describes troubleshooting problems that can occur with an NE2A-series Safety Network Controller.

19-1 Checking the Location of an Error 492
19-1-1 Checking NE2A-series Unit Errors 492
19-1-2 NE2A-series Troubleshooting Procedure 493
19-2 Troubleshooting CPU Unit Errors. 494
19-2-1 Checking the CPU Unit Error Status 494
19-2-2 CPU Unit Error Status and Countermeasures. 496
19-3 Troubleshooting DeviceNet Unit Errors 509
19-3-1 Checking the DeviceNet Unit Error Status. 509
19-3-2 DeviceNet Unit Error Status and Countermeasures 509
19-4 Troubleshooting EtherNet/IP Unit Errors 522
19-4-1 Checking the EtherNet/IP Unit Error Status. 522
19-4-2 EtherNet/IP Unit Error Status and Countermeasure 523
19-5 Troubleshooting Network Configurator Errors. 530
19-5-1 Checking the Network Configurator Error Status 530
19-5-2 Network Configurator Errors and Countermeasures 530
19-6 Connection Status Tables 534
19-6-1 Outline 534
19-6-2 Connection Status for DST1/NE0A Series. 535
19-6-3 Connection Status for the NE1A-series Controller (Safety Slave Function) 538

19-1 Checking the Location of an Error

Errors can occur in the NE2A-series Units, Network Configurator, or Logic Editor.

Error category		Description
NE2A-series Unit errors	CPU Unit • NE2A-SCPU01	Errors that are detected during CPU Unit self-diagnosis or errors that occur in a Communications Unit or I/O Unit connected to the CPU Unit.
	Communications Units • NE2A-DNS21 • NE2A-ENS21	Connection or network errors.
	I/O Units • NE2A-SID4-1 • NE2A-SOD4-1	Safety I/O or test output errors.
Network Configurator errors		Errors that occur when downloading or resetting from a Network Configurator.

19-1-1 Checking NE2A-series Unit Errors

Checking from Indicators on the NE2A-series Controller

The NE2A-series Controllers are designed to indicate errors using individual Unit status indicators or a 7-segment display. Appropriate measures can be taken quickly simply by following the instructions in this manual without using Support Software, such as the Network Configurator.

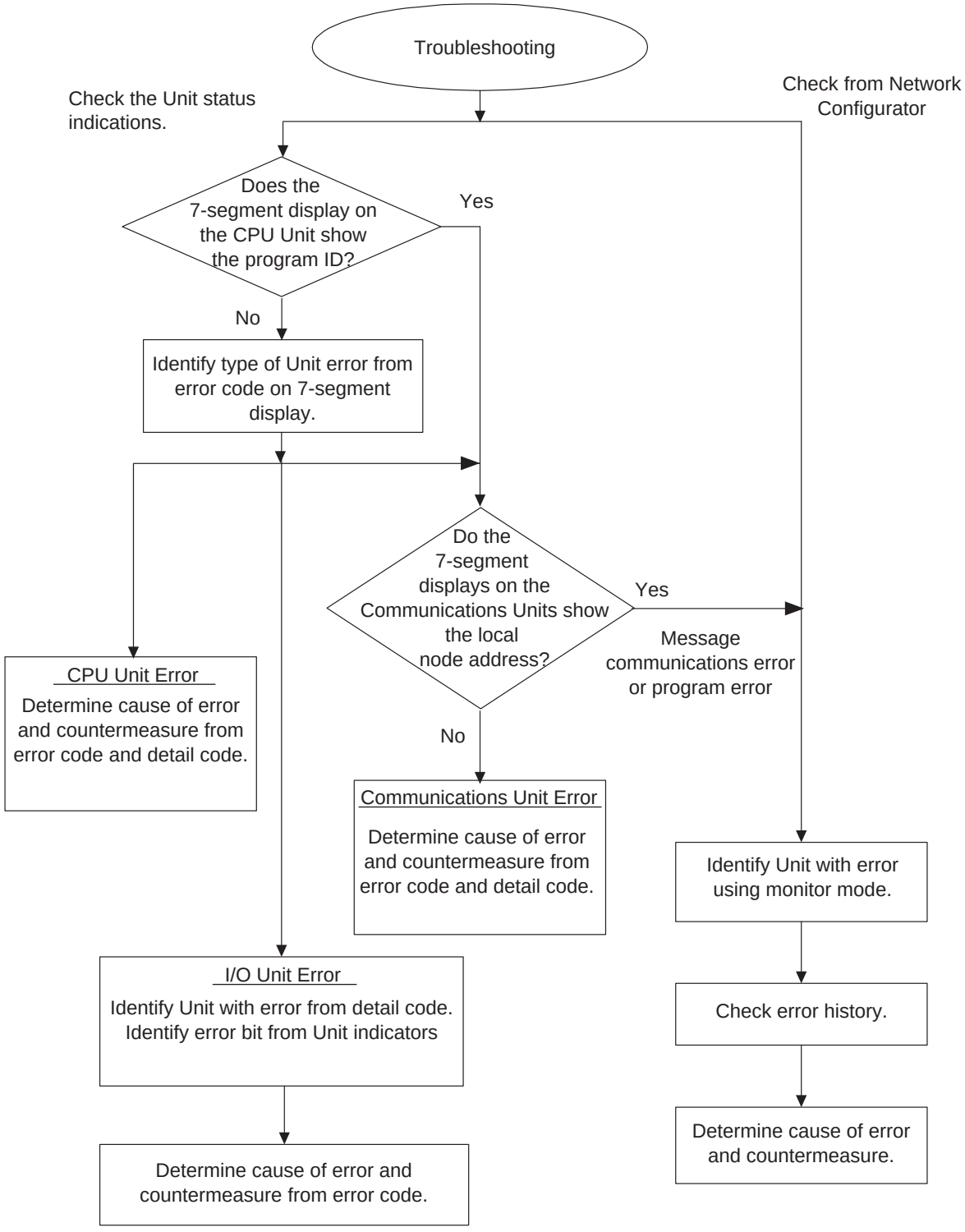
Error history are recorded in the CPU Unit and Communications Units and can be viewed from the Network Configurator.

For details, refer to *19-2 Troubleshooting CPU Unit Errors*, *19-3 Troubleshooting DeviceNet Unit Errors*, and *19-4 Troubleshooting EtherNet/IP Unit Errors*.

Checking from the Network Configurator

The device status can be seen from the Network Configurator by changing the Network Configuration Pane to Maintenance Mode. If alarms or warnings have occurred in the device, the status icon will change to red or yellow. Refer to *9-6-2 Network Configuration Pane* for details.

19-1-2 NE2A-series Troubleshooting Procedure



CPU Unit Errors

Error codes are displayed on the 4-digit 7-segment display on the NE2A-series CPU Unit. The operating status of the CPU Unit, program, and Memory Card are also displayed. Refer to *3-2 Safety CPU Unit* for details on the status indicators.

Alarms and warnings that have occurred in the CPU Unit can be checked from the Network Configurator on the CPU Unit Status Monitor. Refer to *18-2-2 Monitoring Device Status* for details.

Communications Unit Errors

If an error occurs when the NE2A-series Controller is attempting to establish a connection, the error code will be displayed on the 7-segment display on the Communications Unit.

The error status can be checked from the Network Configurator on the DeviceNet Unit Monitor and EtherNet/IP Unit Monitor. Select ***Monitor*** from the Device Menu. Click the **Safety Connections** Tab and check Status. Take the corresponding countermeasure. Safety Communications errors can be observed from the CPU Unit Safety Connections Monitor.

Safety Device Errors

The NE2A-series Safety Input Units and Safety Output Units display the operating status using LED indicators. Refer to *3-8-2 Indicators* for details on Safety Input Units and to *3-9-2 Indicators* for details on Safety Output Units.

Errors occurring at the input terminals, output terminals, or test output terminals can be observed from the CPU Unit Status Monitor. Refer to *18-2-2 Monitoring Device Status* for details.

Network Configurator Execution Errors

These are errors that occur when the NE2A-series Controller is reset, configuration data is downloaded, or the operating mode is changed. The cause of these errors can be determined by checking the error messages displayed in the Message Report Pane of the Network Configurator.

Logic Editor Build Errors

Errors can occur when building program using the NE2A-series Logic Editor. The cause of the error can be determined by checking the error message displayed in the Output Window of the Logic Editor.

19-2 Troubleshooting CPU Unit Errors

19-2-1 Checking the CPU Unit Error Status

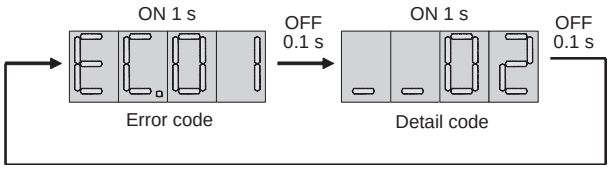
Status Indicators

The status indicators show the status and error codes of a NE2A-series Controller. Refer to *3-2-2 Indicators*.

Seven-Segment Display

The 4-digit 7-segment display shows the status and error codes of a NE2A-series Controller. Refer *3-2-2 Indicators*.

The error code and detail code are displayed alternately.



Error Codes

The upper 2 digits of the error code displayed on the 7-segment display generally indicate the following error categories.

Upper 2 digits of the error code	Error category
C*.	Errors occurring when changing the operating mode with the RUN/STOP/RESTART switch. Errors occurring the configuration restore function. Errors occurring in using the Memory Card. Errors occurring in manipulating the switches.
E*.	Errors related to the configuration.
F*	Fatal errors occurring in the NE2A-series Controller.
H*.	Fatal errors occurring in the NE2A-series Controller.
P*.	Errors related to the I/O Units.
U*.	Errors related to the Communications Units.
-*	Errors related to message communications or the program.

Detail Code

The detail code can be one of three codes: the I/O slot number, Communications Unit number, or a combination of the Communications Unit number and node address. The type of detail code displayed depends on the error code.

Detail code	Meaning
I/O Unit slot number	The I/O Unit slot number is displayed as a 2-digit decimal number. An underscore indicates a blank digit. The slot on the right side of the NE2A-series CPU Unit is slot 1. Slot numbers are assigned to the remaining slots in sequence. There can be up to 20 slots. Example: “_ _ 0 2” indicates slot 2 of the Safety Input Units.
Communications Unit number	The Communications Unit number is displayed as a single digit hexadecimal number. An underscore indicates a blank digit. Example: “_ _ _ A” indicates DeviceNet Unit 10.
Target Unit node address	This code is used when changing the operating mode using the RUN/STOP/RESTART switch or when the system is in RESTORE CONFIGURATION Mode. If an error occurs between the CPU Unit and Target device, the source Communications Unit number will be displayed in the upper 2 digits and the Target node address in the lower 2 digits. The Communications Unit number is displayed as a single digit hexadecimal number. The upper 2 digits and the lower 2 digits are separated by a dot. Example: “_ F. 0 9” indicates that an error occurred at node address 9 which is a device connected to the network though DeviceNet Unit with unit number 15. “--.--” (all hyphens) will be displayed to indicate the CPU Unit.
No display	“----” (4 hyphens) will be displayed if no detail code is used.

Error Categories

When an error occurs in the NE2A-series Controller, operation may be stopped or continued. NE2A-series Controller errors can be categorized into the following three categories.

Error category	Description
Non-fatal Errors	The part where an error has occurred is stopped at each local I/O bit or Safety I/O connection and placed in the safe state. The NE2A-series Controller continues in RUN Mode.
Abort Errors	A non-fatal error such as a CPU Unit configuration mismatch, has occurred. The safety functions will go into the following safe states. • The user logic program will be stopped. • Local Safety Outputs will be turned OFF. • CIP Safety I/O Communications will be stopped. In addition, Standard I/O Communications will stop for Communications Units mounted to the CPU Unit, and only message communications will be enabled.
Critical Errors	A fatal error such as hardware failure or assert error has occurred. The safety functions will go into the following safe states. • The user logic program will be stopped. • Local Safety Outputs will be turned OFF. • CIP Safety I/O Communications will be stopped. In addition, Standard I/O Communications and message communications will be stopped for Communications Units mounted to the CPU Unit, and only message communications from the USB port will be enabled.

19-2-2 CPU Unit Error Status and Countermeasures

Interpreting the Error Status and Countermeasures

The following table describes the abbreviations that appear in the tables of error codes.

Item			Description
CPU Unit	Indicator	MS	Describes the status of the indicator. **Note** No change in display: --
	7-segment display	Error Detail	Gives the error code and detail code displayed on the 7-segment display. Top row: Error code **Note** No display: ---- Bottom row: Detail code **Note** No display: ----

Item			Description
Network Configurator	Error History	Error Detail	Gives the error code and detail code displayed on the 7-segment display. Top row: Error information No display: ---- Bottom row: Detailed information No display: ----
		Saved	Indicates whether a record is saved in the error history. No: No record is saved in error history. Temporary: A record is saved in the error history, but it is deleted when the Unit power is turned OFF. Yes: A record is saved in the error history, and it is not deleted when the Unit power is turned OFF.
	Displayed message		Gives the message displayed in the Error History Monitor Dialog Box of the Network Configurator.
Error name			Names are used to identify errors. Error names are not displayed in the Error History Monitor Dialog Box of the Network Configurator.
Cause Recovery method Status after error			Top row: Cause Gives the cause of the error. Middle row: Reset Gives the method of resetting the error. Bottom row: Status after error Gives the status of the NE2A-series Controller's safety functions after the error has occurred. Refer to *19-1-1 Checking NE2A-series Unit Errors* for details. Abort: Abort fatal error Critical Fault: Critical fault fatal error The status when operation continues is recorded for non-fatal errors.

Critical Errors

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
Lit red	F*.** ****	0601 ****	Yes	System Error.	A system error was detected. Replace the CPU Unit if the error recurs when the Controller is restarted. Operation stops for a critical fault.

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
Lit red	H*.**	0601	Yes	System Error	• The anticipated level of noise was exceeded. • A critical hardware fault occurred.
	****	****			Check the following items. Replace the CPU Unit if the error recurs when the Controller is restarted. • Check the power supply voltage to see if it has dropped or is unstable. • Check whether there is influence from noise, and take whatever corrective actions are required. • Turn the power OFF and back ON and check operation.
					Operation stops for a critical fault.

CPU Unit		Error name	Cause Recovery method Status after error
Indicator	7-segment display		
MS	Error Detail		
Lit red	--.--	System error	A system error was detected.
	****		Replace the CPU Unit if the error recurs when the Controller is restarted.
			Operation stops for a critical fault.

Abort Errors

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
Flashing red	C9.01	2000	Yes	Switch Setting Mismatch.	The MC DOWNLOAD and MC LOCK pins on the Memory Card DIP switch were simultaneously ON when the CPU Unit was started.
	----	0000			Turn OFF one of the pins and restart the CPU Unit.
					Operation is aborted.
Flashing red	EC.01	2001	Yes	I/O Unit number mismatch.	The number of I/O Units in the configuration downloaded to the CPU Unit is different from the actual number of Units installed.
	----	0000			Set the correct configuration and restart the CPU Unit. Alternatively, change and download the NE2A-series Controller parameters.
					Operation is aborted.
Flashing red	EC.02	2002	Yes	I/O Unit configuration mismatch.	The I/O Unit configuration downloaded to the CPU Unit is different from the configuration of the actually installed Units.
	I/O Unit Slot Number	I/O Unit Slot Number			Set the correct configuration and restart the CPU Unit. Alternatively, change and download the NE2A-series Controller parameters.
					Operation is aborted.

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
Flashing Red	EC.11 ----	2003 0000	Yes	Communications Unit number mismatch.	The number of Communications Units in the configuration downloaded to the CPU Unit is different from the actual number of Units installed. Set the correct configuration and restart the CPU Unit. Alternatively, change and download the NE2A-series Controller parameters. Operation is aborted.
Flashing Red	EC.12 Communications unit number	2004 Communications unit number	Yes	Communications Unit configuration mismatch.	The Communications Unit configuration downloaded to the CPU Unit is different from the configuration of the actually installed Unit. Set the correct configuration and restart the CPU Unit. Alternatively, change and download the NE2A-series Controller parameters. Operation is aborted.
Flashing Red	EC.13 Communications unit number	2005 Communications unit number	Yes	Communications Unit configuration mismatch.	The Communications Unit configuration ID downloaded to the CPU Unit is different from the actual Communications Unit ID. Set the correct configuration and restart the CPU Unit. Alternatively, change and download the NE2A-series Controller parameters. Operation is aborted.
Flashing Red	Ed.01 ----	2006 0000	Yes	Number of I/O Units connected has exceeded the limit.	The number of I/O Units connected to the CPU Unit has exceeded the limit. (Up to 20 Units can be connected.) Set the correct configuration and restart the CPU Unit. Operation is aborted.
Flashing Red	Ed.02 ----	2007 0000	Yes	End Unit not connected.	The End Unit is not connected to the right of the CPU Unit. Set the correct configuration and restart the CPU Unit. Operation is aborted.
Flashing Red	Ed.11 ----	2008 0000	Yes	Number of Communications Units connected has exceeded the limit (Without Power Supply Unit).	More than three Communications Units are connected but a Power Supply Unit is not connected. Connect no more than three Communications Units and restart the CPU Unit. Alternatively, connect a Power Supply Unit and restart the System. Operation is aborted.
Flashing Red	Ed.12 ----	2009 0000	Yes	Number of Communications Units connected has exceeded the limit (With Power Supply Unit).	More than six Communications Units are connected when a Power Supply Unit is connected. Connect no more than six Communications Units and restart the CPU Unit. Operation is aborted.

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
Flashing red	Ed.15 ---- I/O Unit Slot Number	200C 0000 I/O Unit Slot Number	Yes	Power supply adapter not connected.	A CJ-series CPU Unit, CJ-series I/O Control Unit (CJ1W-IC101), or CJ-series I/O Interface Unit (CJ1W-II101) is mounted. Set the correct configuration and restart the CPU Unit. Replace the Power Supply Unit, Communications Unit, or CPU Unit if the error recurs. Operation is aborted.
Flashing red	EE.01 I/O Unit Slot Number	200D I/O Unit Slot Number	Yes	Incorrect I/O Unit connected.	The type of I/O Unit that is mounted is not defined. Change the I/O Unit and restart the CPU Unit. Operation is aborted.
Flashing red	EE.02 I/O Unit Slot Number	200E I/O Unit Slot Number	Yes	Allocated I/O Unit address mismatch.	An error occurred in setting an address for an I/O Unit at startup. Replace the I/O Unit and restart the CPU Unit. Operation is aborted.
Flashing red	EE.03 I/O Unit Slot Number	200F I/O Unit Slot Number	Yes	I/O Unit configuration failed.	An error occurred in setting the configuration of an I/O Unit at startup. Replace the I/O Unit and restart the CPU Unit. Operation is aborted.
Flashing red	EE.04 I/O Unit Slot Number	2014 I/O Unit Slot Number	Yes	I/O Unit configuration failed.	An error occurred because the configuration data for an I/O Unit was incorrect at startup. Download the parameters and restart the I/O Unit. If the problem recurs, replace the I/O Unit and restart. Operation is aborted.
Flashing red	EE.11 Communications unit number	2010 Communications unit number	Yes	Communications Unit not supported.	A Communications Unit that is not supported by the NE2A-series Controller is connected. Remove the Communications Unit and restart the CPU Unit. Operation is aborted.
Flashing red	EE.12 Communications unit number	2011 Communications unit number	Yes	Invalid Unit Number.	The Communications Unit number is outside the valid range. Correct the unit number setting and restart the CPU Unit. Operation is aborted.
Flashing red	EE.13 Communications unit number	2012 Communications unit number	Yes	Duplicate Unit Number.	The same Communications Unit number is set for two different Units. Correct the unit number setting and restart the CPU Unit. Operation is aborted.
Flashing red	EE.14 Communications unit number	2013 Communications unit number	Yes	Communications Unit Connection Error.	The Communications Unit could not be correctly recognized. “H4” or “H5” may be displayed on 7-segment display on the DeviceNet Unit. If there is an error in the Communications Unit, remove the cause of the error and restart. If the error recurs, replace the Communications Unit and CPU Unit. Operation is aborted.

Errors Related to Operation of the RUN/STOP/RESTART Switch, 1/2

CPU Unit		Error name	Cause Recovery method Status after error
Indicator	7-segment display		
MS	Error Detail		
Flashing green/red	C2.13 Target node address	Error with downloaded parameters.	The configuration cannot be restored because there was an error in the parameters downloaded to the Target device.
			Check the Target device. Alternatively, check the operation rights file and recreate it if it is different from the network configuration.
			Operation continues for the next device.

Errors Related to Operation of the RUN/STOP/RESTART Switch, 2/2

CPU Unit		Error name	Cause Recovery method Status after error
Indicator	7-segment display		
MS	Error Detail		
--	C1.01 Target node address	Communications timeout.	A request for changing the mode or restoring the configuration timed out because a Target device was missing or because of an error in the communications path. (See note.)
			Check the Target device and other devices that form the communications path. Alternatively, check the operation rights file and recreate it if it is different from the network configuration.
			Operation continues for the next device.
--	C1.02 Target node address	Error Occurred on Communications path.	A mode change or configuration restoration cannot be executed because an error occurred in the Communications Unit mounted or in a device that forms the communications path. (See note.)
			Check the status of the Communications Unit. If an error has occurred, reset it and execute the operation again.
			Operation continues for the next device.
--	C2.01 Target node address	Vendor ID Error.	A mode change or configuration restoration cannot be executed because the vendor ID of the Target device does not match. (See note.)
			Check the Target device. Alternatively, check the operation rights file and recreate it if it is different from the network configuration.
			Operation continues for the next device.
--	C2.02 Target node address	Device Type Error.	A mode change or configuration restoration cannot be executed because the Target device type does not match. (See note.)
			Check the Target device. Alternatively, check the operation rights file and recreate it if it is different from the network configuration.
			Operation continues for the next device.
--	C2.03 Target node address	Product Code Error.	A mode change or configuration restoration cannot be executed because the device product code does not match. (See note.)
			Check the Target device. Alternatively, check the operation rights file and recreate it if it is different from the network configuration.
			Operation continues for the next device.

CPU Unit		Error name	Cause Recovery method Status after error
Indicator	7-segment display		
MS	Error Detail		
--	C2.04 Target node address	Revision Mismatch	The operating mode cannot be changed or the configuration cannot be restored because the major revision of the device was lower (i.e., older) than the major revision of the device registered in the configuration restore file. This error message will be displayed only ten times if the error occurs when changing the operating mode using the RUN/STOP/RESTART switch. The display will be held if the error occurs when restoring the configuration.
			Check the Target device. Alternatively, check the configuration restore file and make sure the device revisions are the same.
			Operation continues for the next device.
--	C2.05 Target node address	TUNID Mismatch.	An operating mode change or configuration restoration cannot be executed because the TUNID of the Target device does not match. (See note.)
			Check the Target device. Alternatively, check the operation rights file and recreate it if it is different from the network configuration.
			Operation continues for the next device.
--	C2.06 Target node address	Device Password Error.	The operating mode cannot be changed or the configuration cannot be restored because the password of the Target device does not match. (See note.)
			Check the Target device. Alternatively, check the operation rights file and recreate it if it is different from the network configuration.
			Operation continues for the next device.
--	C2.07 Target node address	Status Error.	The operating mode cannot be changed or the configuration cannot be restored because the Target device is in an error state or at least not in a state that allows changing the mode. (See note.)
			Check the Target device. Alternatively, check the operation rights file and recreate it if it is different from the network configuration.
			Operation continues for the next device.

Note The mode will be displayed for 30 seconds only when changing the operating mode using the RUN/STOP/RESTART switch. The display remains for the entire duration while configuration is being restored.

Errors Related to Operations with a Memory Card

CPU Unit		Error name	Cause Recovery method Status after error
Indicator	7-segment display		
MS	Error Detail		
--	C3.01 ----	The configuration restore files is not validated.	The operating mode cannot be changed or the configuration cannot be restored because the authenticity of the configuration restore file has not been confirmed or a Memory Card is not inserted.
			The error display will disappear when a Memory Card is inserted. Confirm the configuration restore file after this occurs. Use the following procedure to check the configuration restore file.
			The relevant function is not executed, and other operations continue. If the RUN/STOP/RESTART switch is pressed while the configuration restore file is being checked (i.e., while the file ID is displayed), this error will be displayed for 10 s, and then the file ID will be displayed again, and the system will wait for user confirmation (i.e., until the SERVICE switch is pressed). If the system is in CONFIGURATION RESTORE Mode and the Memory Card is not inserted, the system will wait for the Memory Card to be inserted.
--	C3.02 ----	Memory Card removed during operation.	The process cannot be continued because power supplied to the Memory Card was turned OFF or the Memory Card was removed when the operating mode was being changed or the configuration was being restored. (See note 1.)
			Insert the Memory Card and reconfirm the configuration restore file. **Note** The error display will disappear when the Memory Card is inserted. Use the following procedure to check the configuration restore file.
			If the operating mode is changed using the RUN/STOP/RESTART switch, only processing the operating mode change will stop. Other operations will continue. In CONFIGURATION RESTORE Mode, processing in progress will be stopped, and the system will wait for the Memory Card to be inserted again. (When the Memory Card is inserted, configuration restore operation will continue again from the start.)
--	C3.03 ----	Configuration restore file not found on Memory Card	The configuration restore file cannot be confirmed because it cannot be found in the Memory Card.
			Insert a Memory Card with the configuration restore file. **Note** The error display will disappear when the Memory Card is inserted.
			The relevant function is not executed, and other operations continue.
--	C3.05 ----	Configuration restore file read error	The configuration restore file cannot be confirmed because it cannot be read properly from the Memory Card.
			Check the Memory Card and confirmation restore file. Insert a Memory Card with the correct confirmation restore file. **Note** The error display will disappear when the Memory Card is removed.
			The relevant function is not executed, and other operations continue

CPU Unit		Error name	Cause Recovery method Status after error
Indicator	7-segment display		
MS	Error Detail		
--	C3.06 ----	Invalid configuration restore file data	The configuration restore file cannot be confirmed because the check code of the configuration restore file read from the Memory Card is incorrect.
			Check the Memory Card and configuration restore file. Insert a Memory Card with the correct configuration restore file. **Note** The error display will disappear when the Memory Card is removed.
			The relevant function is not executed, and other operations continue.
--	C8.01 ----	Switch changed during operation.	Either the MC DOWNLOAD or MC LOCK pin on the Memory Card DIP switch was turned ON during operation. **Note** Turning OFF the DIP switch pin in CONFIGURATION RESTORE Mode will not affect operation.
			Change the switch pin back to OFF. **Note** The error display will disappear when the pin is turned OFF.
			The error will be displayed only. Operation will continue.
--	CA.01 ----	Switch Failure.	The RUN/STOP/RESTART switch setting is invalid. (The switch setting is not applicable.) The error is displayed only. It does not affect operation. The RUN/STOP/RESTART switch operation will be ignored.
			Restart the CPU Unit. Replace the CPU Unit if the error recurs when the Controller is restarted.
			The error will be displayed only. Operation will continue.

Errors Related to Configuration

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
--	E9.01 ----	0012 (Refer to Cause)	Yes	Non-volatile Memory Error.	One of the following Standard Parameter errors was detected despite the configuration being completed. Error history detailed information: 0001: CPU Unit system setting (Standard Parameters only) 0002: Name information 0003: Arrangement information for programs
					Download the parameters to the NE2A-series Controller again. Replace the CPU Unit if the error recurs.
					Operation continues with the default values for the applicable configuration data.
--	E9.02 ----	0012 0011	Yes	Non-volatile Memory Error.	A Unit ON time error occurred or the memory area for saving the Unit ON time cannot be used.
					Restart the CPU Unit. Replace the CPU Unit if the error recurs.
					Operation continues with 0 as the Unit ON time.

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
--	E9.03	0012	Temporary	Non-volatile Memory Error.	None of the areas for saving the error history can be used.
	----	0021			Restart the CPU Unit. Replace the CPU Unit if the error recurs.
					Only the error history data in RAM is updated, and operation continues. This error is saved only to RAM.
--	E9.04	0012	Yes	Non-volatile Memory Error.	None of the areas for saving the operating history can be used.
	----	0031			Restart the CPU Unit. Replace the CPU Unit if the error recurs.
					Only the operating history data in RAM is updated, and operation continues.
--	E9.05	0012	Yes	Non-volatile Memory Error.	An error was detected in the maintenance information.
	----	0041			Restart the CPU Unit. Replace the CPU Unit if the error recurs.
					Operation continues with 0 as the number of ON times for the terminals where the error occurred.
--	E9.06	0012	Yes	Non-volatile Memory Error.	An error occurred when saving or reading the configuration restore file confirmation information.
	----	0061			Restart the CPU Unit. Replace the CPU Unit if the error recurs.
					Operation continues with the configuration restore file being authenticated. The configuration restore file cannot authenticated in Configuration Restore Mode, so downloading and locking the configuration are not possible.
--	E9.11	0012	Yes	Non-volatile Memory Error.	A Safety Parameter error was detected despite the configuration being completed.
	----	0061			Reset the NE2A-series Controller to the default parameters and then download the parameters again. Replace the CPU Unit if the error recurs.
					Operation continues waiting for configuration. The error will be cleared when the configuration is completed.

Errors Related to I/O Units

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
--	P1.02 I/O Unit slot number	2052 I/O Unit slot number	Yes	External Test Signal Failure at Safety Input.	A test pulse error was detected at the Safety Input terminal. (It was disconnected or there was an error in a connected device.) Alternatively, an error was detected at the test output terminal associated with a Safety Input. (Overcurrent was detected or the output was stuck at high.)
					Check the external input devices and the wiring and remove the cause of the error. Input OFF to the input terminal after the error latch time has passed.
					CPU Unit operation continues. At the applicable I/O Unit, the I/O indicator lights red for the terminal where the error occurred. When dual channels are set, the I/O indicator for the other terminal flashes red.

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
--	P1.03 I/O Unit slot number	2053 I/O Unit slot number	Yes	Internal Input Failure at Safety Input.	An error was detected in the internal circuit of the Safety Input terminal. Input OFF to the input terminal after the error latch time has passed. Replace the I/O Unit if the error recurs. CPU Unit operation continues. At the applicable I/O Unit, the I/O indicator lights red for the terminal where the error occurred. When dual channels are set, the I/O indicator for the other terminal flashes red.
--	P1.04 I/O Unit slot number	2054 I/O Unit slot number	Yes	Discrepancy Error at Safety Input.	A logic error was detected between the Safety Input terminals of a dual channel. Review the discrepancy time and download new settings. CPU Unit operation continues. At the applicable I/O Unit, the I/O indicators light red for the pair of dual channel terminals where the error occurred.
--	P3.03[k3] I/O Unit slot number	2063 I/O Unit slot number	Yes	Short Circuit Detected at Safety Output.	A short-circuit was detected at the Safety Output terminal. Check the Safety Output terminal wiring and remove the cause of the error. Output OFF from the output terminal after the error latch time has passed. CPU Unit operation continues. At the applicable I/O Unit, the I/O indicator lights red for the terminal where the error occurred. When dual channels are set, the I/O indicator for the other terminal flashes red.
--	P3.04 I/O Unit slot number	2064 I/O Unit slot number	Yes	Stuck-at-high Stuck-at-high Detected at Safety Output.	The Safety Output terminal is stuck at high. Check the Safety Output terminal wiring and remove the cause of the error. Output OFF from the output terminal after the error latch time has elapsed. CPU Unit operation continues. At the applicable I/O Unit, the I/O indicator lights red for the terminal where the error occurred. When dual channels are set, the I/O indicator for the other terminal flashes red.
--	P3.08 I/O Unit slot number	2068 I/O Unit slot number	Yes	Dual Channel Violation Dual Channel Violation at Safety Output.	A logic error was detected between the Safety Output terminals of a dual channel. Check the Safety Output terminal wiring and remove the cause of the error. Output OFF from the output terminal after the error latch time has elapsed. CPU Unit operation continues. At the applicable I/O Unit, the I/O indicators light red for the pair of dual channel terminals where the error occurred.
--	P4.01 I/O Unit slot number	2070 I/O Unit slot number	Yes	Input PS Voltage Low.	Power is not supplied to the Input Unit. Check the power supply and the wiring. CPU Unit operation continues. At the applicable I/O Unit, none of the I/O indicators are lit.
--	P5.01 I/O Unit slot number	2071 I/O Unit slot number	Yes	Output PS Voltage Low.	Power is not supplied to the Output Unit. Check the power supply and the wiring. CPU Unit operation continues. At the applicable I/O Unit, none of the I/O indicators are lit.

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
--	P6.01 I/O Unit slot number	2072 I/O Unit slot number	Yes	I/O Power Supply Shutdown Error.	An error was detected during the output shutdown test of the Output Unit.
					Check the wiring. Replace the I/O Unit if the error recurs despite correct wiring.
					CPU Unit operation continues. At the applicable I/O Unit, the TS indicator lights red and operation stops.
--	PA.01 I/O Unit slot number	2073 I/O Unit slot number	Yes	Slice Bus Communications Error.	A timeout was detected during Safety I/O Communications or Standard Communications with the I/O Unit.
					Replace the I/O Unit if the error recurs when the Controller is restarted
					CPU Unit operation continues. At the applicable I/O Unit, the TS indicator lights red and operation stops.
--	PF.01 I/O Unit slot number	2074 I/O Unit slot number	Yes	I/O Unit System Error.	An error was detected during self-diagnosis by the I/O Unit.
					Replace the I/O Unit if the error recurs when the Controller is restarted
					CPU Unit operation continues. At the applicable I/O Unit, the TS indicator lights red and operation stops.

Errors Related to Communications Units

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
--	UE.01 ---- 0000	2080	Yes	Communications Unit Bus Error.	An error was detected during the bus check for the Communications Unit.
					Check the power supply voltage of the NE2A-PD025 Power Supply Unit to see if it has dropped or is unstable.
					CPU Unit operation continues. Servicing stops for all Communications Units, so all Safety I/O Communications and Standard I/O Communications stop.
--	UF.01 Communications	2081 Communications	Yes	Communications Unit watchdog timer Timeout.	The Communications Unit stopped after a watchdog timer error.
					Check the power supply voltage of the NE2A-PD025 Power Supply Unit to see if it has dropped or is unstable.
					CPU Unit operation continues. Servicing stops for the applicable Communications Unit, so Safety I/O Communications and Standard I/O Communications through that Unit stop.

Errors Related to the Program

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
--	----	2090 0000	Yes	Function block error.	A logic error was detected in a function block of the user program.
					The way to cancel the error depends on the function block. If the error recurs, review the discrepancy time, set the program execution delay, and download the new settings. *Safety Network Controller Command Reference Manual* (Cat. No. Z920)
					CPU Unit operation continues. The PERR indicator lights red.

Errors Related to Message Communications

CPU Unit		Network Configurator			Cause Recovery method Status after error
Indicator	7-segment display	Error history		Displayed message	
MS	Error Detail	Error Detail	Saved		
--	----	0118 0000	Yes	Discard Invalid Message.	An invalid message was received and discarded. (Response could not be returned due to invalid format.)
					--
					Operation continues.
--	----	0119 0000	Yes	Busy Message discarded.	The message was discarded because the CPU Unit was busy. (Response could not be returned due to invalid format.)
					Reduce the load on the CPU Unit.
					Operation continues.

19-3 Troubleshooting DeviceNet Unit Errors

19-3-1 Checking the DeviceNet Unit Error Status

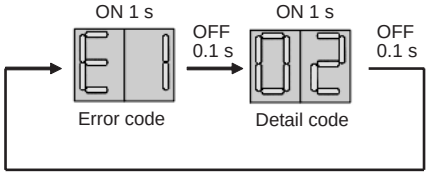
Status Indicator

The status indicators show the status and error codes of a DeviceNet Unit. Refer to *3-6-2 Indications*.

Seven-Segment Display

The 2-digit 7-segment display shows the status and error codes of a DeviceNet Unit. Refer to *3-6-2 Indications*.

The error code and detail code are displayed alternately.



Error Code

The 2 digits of the 7-segment display generally indicate the following error categories.

Error code	Error category
OFF	System errors related to the DeviceNet Unit.
A*	Errors related to the Safety I/O Communications.
C*	Errors related to switch operation.
d*	Errors related to the Master.
E*, F*	Errors related to the network.
H*	Errors related to interaction with the CPU Unit.
L*	Errors related to the Slave.
--	Errors related to message communications.

19-3-2 DeviceNet Unit Error Status and Countermeasures

Interpreting the Error Status and Countermeasures

The following table describes the abbreviations that appear in the tables of error codes.

Item			Description
Communications Unit (DeviceNet Unit)	Indicators	MS NS	Gives the status of the MS and NS indicators. Top row: MS indicator **Note** No change in display: -- Bottom row: NS indicator **Note** No change in display: --
	7-segment display	Error Detail	Gives the error code and detail code displayed on the 7-segment display. Top row: Error code Bottom row: Detail code

Item			Description
Network Configurator	Error History	Error Detail	Gives the error and detailed information recorded in the error history table. (Information displayed in the Error History Monitor Dialog Box.) Top row: Error code ----: Not recorded in error history. (Not saved in error history table.) Bottom row: Detailed code ----: Not recorded in error history. (Not saved in error history table.)
		Saved	Indicates whether a record is saved in the error history. No: No record is saved in error history. Yes: A record is saved in the error history, but it is deleted when the Unit power is turned OFF. Temporary: A record is saved in the error history, and it is not deleted when the Unit power is turned OFF.
	Displayed message		Gives the message displayed in the Safety Connections Monitor Dialog Box.
Error name			Names are used to identify errors. Error names are not displayed in the Error History Monitor Dialog Box of the Network Configurator.
Cause Recovery method Status after error			Top row: Cause Gives the cause of the error. Middle row: Reset Gives the method of resetting the error. Bottom row: Status after error Gives the status of the DeviceNet Unit after the error has occurred.

System Errors Related to the DeviceNet Unit

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
Lit red OFF	OFF	0601 ***	Yes	Special Unit Error.	A DeviceNet Unit hardware error has occurred. Replace the DeviceNet Unit if the error recurs when the Controller is restarted is restarted. Operation stops.

Communications Unit		Error name	Cause Recovery method Status after error
Indicators	7-segment display		
MS NS	Error Detail		
Lit red OFF	OFF	Special Unit Error.	A DeviceNet Unit hardware error occurred. Replace the DeviceNet Unit if the error recurs after the Controller is restarted. Operation stops.

Communications Unit		Error name	Cause Recovery method Status after error
Indicators	7-segment display		
MS NS	Error Detail		
Lit red	H3	Special Unit Error.	A DeviceNet Unit hardware error occurred.
OFF	---		Replace the DeviceNet Unit if the error recurs after the Controller is restarted.
			Operation stops.

Hardware Setting Errors for DeviceNet Units

Communications Unit		Error name	Cause Recovery method Status after error
Indicators	7-segment display		
MS NS	Error Detail		
Flashing red	H0	CPU Unit connection error with unsupported device.	The DeviceNet Unit is connected to a CPU Unit that does not support it.
	---		Check the CPU Unit. Mount the DeviceNet Unit properly.
OFF			Operation stops.
Flashing red	H1	Unit Number Setting Error.	The DeviceNet Unit number setting is the same as the number setting of another Unit.
	---		Set the number so that it does not the same as the number of another Unit. "EC.13" may be displayed on the 7-segment display on the CPU Unit.
OFF			Operation stops. Monitoring with the Network Configurator is not possible.
Flashing red	H2	CPU Unit faulty.	An error occurred in the CPU Unit.
	---		Replace the CPU Unit if the error recurs when the Controller is restarted.
OFF			Operation stops.
Flashing red	H4	Node address setting error.	There is an error in the node address switch setting. (There is a value that exceeds 63.)
	---		Set the node address to within a valid range (63 or lower) and restart the power supply.
OFF			Operation stops.
Flashing red	H5	Baud Rate Setting Error.	There is an error with the baud rate setting.
	---		Correct the baud rate setting and restart the power supply.
OFF			Operation stops.

CPU Unit Errors for DeviceNet Units

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
Flashing red OFF	H6 ---	000F 0000	Yes	CPU Unit faulty.	An error occurred in the CPU Unit. Replace the DeviceNet Unit or CPU Unit if the error recurs when the Controller is restarted. Operation stops.
Flashing red OFF	H7 ---	0006 Bit 6 ON: Duplicated unit number Bit 3 ON: No applicable device number in registered I/O tables + 00	Yes	I/O table not registered.	The unit number is not registered in the CPU Unit I/O tables. Create the I/O tables. Operation stops.

Setting Errors for DeviceNet Units

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
Flashing red --	C8 Local node address	0349 02: Node address rotary switch changed 03: Baud rate DIP switch changed + Value before switch was changed (value when power was applied)	Yes	Switch changed during operation.	The hardware switch setting was changed during operation. Reset the settings to what it was before the change was made. Alternatively, restart the DeviceNet Unit after the change is made. Safety I/O Communications will be stopped. Standard I/O Communications and other operations will be continued. Safety I/O Communications will be restarted if the switch setting is reset to its original setting.
Flashing red --	E6 Local node address	021A 000E	Yes	Logic error in configuration data.	There is an error with the unit name saved in the non-volatile memory. Reset the unit name with the Configurator. Replace the DeviceNet Unit if the error recurs. Operation continues with the unit name as null. Other functions are also continued.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
Flashing red --	E8 Local node address	021A 000A	Yes	Logic error in configuration data.	There is an error with the Master scan list saved in the non-volatile memory. Register the scan list again after clearing it. Alternatively, reset the Master scan list with the Network Configurator. 1) Master remote I/O communications will be stopped. 2) Data exchange with the CPU Unit, operation as a Slave, and message communications will be continued. After this, the system will return to normal operation if the data can be correctly written. (Remote I/O communications will be performed for the Master.)
Flashing red --	E9 Local node address	0602 ****	Yes*1	Memory access error.	An error occurred when reading/writing to the non-volatile memory in the Unit. A record may not be saved in the error history in some cases Replace the DeviceNet Unit if the error recurs. Writing to non-volatile memory is ignored and operation continues.
Flashing red --	Hb Local node address	0011 ****	Yes	CPU Unit event servicing time-out.	A timeout occurred while reading parameters to the CPU Unit. Replace the DeviceNet Unit and/or the CPU Unit if the error recurs when the Controller is restarted. Operation continues as if the error information is not set.
Flashing red --	HC Local node address	021A ****	Yes	Logic error in configuration data.	There is an error with the CPU Unit configuration data setting. “EC.11,” “EC.12,” “Ed.15,” or “EE.11” may be displayed on the 7-segment display on the CPU Unit. Download the configuration data again. Replace the DeviceNet Unit or the CPU Unit if the error recurs. Operation continues as if the error information is not set.
Flashing red --	HE Local node address	0002 Monitoring time (ms)	Yes	CPU Unit service monitoring error.	Service from the CPU Unit is disabled for a period. Monitoring is normally for 11 s. Review the CPU Unit operation environment. Replace the DeviceNet Unit or CPU Unit if the error recurs. Processes other than Safety I/O and Standard I/O are continued. Safety I/O and Standard I/O will be restarted when servicing from the CPU Unit is restarted.
Flashing red --	HF Local node address	0001 0000	No	CPU Unit watchdog timer error.	An error occurred in the CPU Unit. Check for the presence of noise, and remove the noise source. Replace the CPU Unit if the error recurs. Interaction with the CPU Unit will be stopped, Safety and Standard I/O Communications will be stopped, and all other functions will be continued.

Communications Errors for DeviceNet Units

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
-- OFF	E0 Local node address	0341 0000	Yes	Network PS Voltage Low.	The power supply from the network is not provided properly. Check the network power supply and the network cable wiring. • The Unit will be offline and communications will be disabled. An error will be returned for all communications requests. • Data exchange with the CPU Unit will be continued.
-- OFF/Flashing Red (See note.)	E2 Local node address	0342 0000	Yes	Transmission Timeout.	The transmission request was not completed successfully due to the following reasons. • There are no Slave devices on the network. • The baud rate setting is different between nodes. • There was an error with the CAN Controller. Consider the following items. • The baud rates for the Master and Slaves may not be the same. • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise? Remote I/O communications will be stopped while transmission is timed out. An error will be returned for message transmission requests. Communications will be restarted when the DeviceNet Unit recovers from the transmission timeout.
-- . Lit red	F0 Local node address	0211 00 + Duplicated node address	Yes	Duplicate MAC ID.	The same node address is set for another node. (Occurs when going online.) Check the node addresses of the other devices. Make sure that there is no duplication and restart the DeviceNet Unit. • The Unit will be offline and communications will be disabled. An error will be returned for all communications requests. • Data exchange with the CPU Unit will be continued.
-- Lit red	F1 Local node address	0340 0000	Yes	Bus Off.	A Bus Off error was detected. Consider the following items. • Are the baud rates for the Master and Slaves the same? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise? • The Unit will be offline and communications will be disabled. An error will be returned for all communications requests. • Data exchange with the CPU Unit will be continued

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
-- Flashing red	A1 Target node address	2100 00 + Safety Slave node address	Yes	Part of the System stopped due to Safety I/O Communications error.	The Safety Master connection supported by the DeviceNet Unit was disconnected while part of the System was stopped due to a Safety I/O Communications error.
					Establish communications from the Network Configurator again.
					The Safety I/O Connection where the error occurred will remain stopped without establishing the connection again. Any other operations will be continued.
-- Flashing red	d5 Target node address	0344 01 + Slave node address	Yes	Verification errors (Standard I/O).	No Standard Slaves exist in the network when the Standard Master connection is established.
					Consider the following items. • Is the Standard Slave power supply OFF? • Is the Standard Slave node address correct? • Are the baud rates for the Standard Master and Standard Slaves on the network the same? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise?
					Repeated attempts will be made to establish the Standard I/O Connection again. Other operations will be continued.
-- Flashing red	d5 Target node address	2101 2C + Safety Slave node address	Yes	Nonexistent Safety Slave Device.	No Safety Slaves exist in the network when the Safety Master connection is established.
					Consider the following items. • Is the Safety Slave power supply OFF? • Is the Safety Slave node address correct? • Are baud rates for the Standard Master and Standard Slaves on the network the same? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise?
					Repeated attempts will be made to establish the Standard I/O Connection again. Other operations will be continued.
-- Flashing Red	d6 Target node address	2101 01 to 68 + Safety Slave node address	Yes	I/O Connection Establishment Failure.	The Safety Slave device configuration is invalid or Safety I/O Communications is disabled while a Safety Master connection is being established.
					Consider the following items. • Is the Safety Slave MAC ID correct? • Is the Safety Slave configuration correct? • Is the Safety Slave operating mode correct?
					Repeated attempts will be made to establish the Standard I/O Connection again. Other operations will be continued.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
-- Flashing red	d6 Target node address	0344 02 + Slave node address	Yes	Verification errors (Standard I/O).	The Slave vendor ID does not match with the vendor ID registered in the scan list. Check that the communications target Slave is set correctly and that the vendor ID registered in the scan list is correct. Correct the settings if necessary. Repeated attempts will be made to establish the Standard I/O Connection again. Other operations will be continued.
-- Flashing Red	d6 Target node address	0344 03 + Slave node address	Yes	Verification errors (Standard I/O).	The Slave device type does not match what is registered in the scan list. Check that the communications Target Slave is set correctly and that the Slave device type registered in the scan list is also correct. Correct the settings if necessary. Repeated attempts will be made to establish the Standard I/O Connection again. Other operations will be continued.
-- Flashing red	d6 Target node address	0344 04 + Slave node address	Yes	Verification errors (Standard I/O).	The Slave product code does not match what is registered in the scan list. Check that the communications Target Slave is set correctly and that the Slave product code registered in the scan list is also correct. Correct the settings if necessary. Repeated attempts will be made to establish the Standard I/O Connection again. Other operations will be continued.
-- Flashing red	d6 Target node address	0344 05 + Slave node address	Yes	Verification errors (Standard I/O).	The I/O connection registered in the scan list is not supported by the device. Check that the communications Target Slave is set correctly and that the connection registered in the scan list is also correct. Correct the settings if necessary. Repeated attempts will be made to establish the Standard I/O Connection again. Other operations will be continued.
-- Flashing red	d6 Target node address	0344 06 + Slave node address	Yes	Verification errors (Standard I/O).	The Slave I/O data size does not match what is registered in the scan list. Check that the communications Target Slave is set correctly and that the connection registered in the scan list is also correct. Correct the settings if necessary. Repeated attempts will be made to establish the Standard I/O Connection again. Other operations will be continued.
-- Flashing red	d6 Target node address	0344 07 + Slave node address	Yes	Verification errors (Standard I/O).	A connection path registered in the scan list could not be set. Check that the communications Target Slave is set correctly and that the Slave connection bus setting registered in the scan list is also correct. Correct the settings if necessary. Repeated attempts will be made to establish the Standard I/O Connection again. Other operations will be continued.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
--	d9	0345	Yes	Standard I/O Connection Timeout.	A timeout occurred during remote I/O communications with the Master.
Flashing red	Target node address	01 + Slave node address			Consider the following items. • Is the Standard Slave power supply OFF? • Are baud rates for the Standard Master and Standard Slaves on the network the same? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise?
					Repeated attempts will be made to establish the Standard I/O Connection again. Other operations will be continued.
--	dA	2102	Yes	Safety I/O Connection Timeout.	A communications timeout occurred during Safety I/O Communications with the Slave device.
Flashing red	Target node address	01 + Safety Slave node address			Consider the following items. • Is the Safety Slave node address correct? • Is the Safety Slave configuration correct?
					The recovery method depends on the setting for when an error occurs in Safety Communications. • Connection Stop Mode The Safety I/O Connection where the error occurred will be stopped. • Automatic Recovery Mode Repeated attempts will be made to establish the Safety I/O Connection again. All other operations will be continued.
--	E2	0342	Yes	Transmission Timeout.	Due to the following reasons, the transmission request was not completed successfully. • There are no Slaves on the network. • The baud rate setting is different between nodes. • There was an error with the CAN Controller.
OFF/Flashing red (See note.)	Local node address	0000			Consider the following items. • Are baud rates for the Standard Master and Standard Slaves on the network the same? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise?
					Remote I/O communications will be stopped while transmission is timed out. Message transmission requests will be returned with an error. Communications will be restarted when the DeviceNet Unit recovers from the transmission timeout.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	**7-segment display**	**Error history**		**Displayed message**	
MS **NS**	**Error** **Detail**	**Error** **Detail**	**Saved**		
-- Flashing red	L9 Target node address	0345 02 + Master node address	Yes	Standard I/O Connection Timeout.	A timeout occurred during remote I/O communications with the Slave.
					Consider the following items. • Is the Master functioning properly? • Are baud rates for the Standard Master and Standard Slaves on the network the same? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise?
					An error will be returned for communications requests to the Master with the error. Data output to the CPU Unit (i.e., data from the Master) is cleared. Communications can be restarted by reconnecting to the Master.
-- Flashing red	LA Target node address	2102 01 + Safety Master node address	Yes	Safety I/O Connection Timeout.	A communications timeout occurred during Safety I/O Communications with the Master device.
					Consider the following items. • Is the Safety Master node address correct? • Is the Safety Master configuration data correct?
					The recovery method depends on the setting for when an error occurs in Safety Communications. • Connection Stop Mode The Safety I/O Connection where the error occurred will be stopped. • Automatic Recovery Mode Repeated attempts will be made to establish the Safety I/O Connection again. All other operations will be continued.

Note Errors occurring during I/O communications result in the indicator flashing red. In any other situation the indicator is OFF.

Errors Related to Explicit Message Communications

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
--	--	0101	Temporary	Transmission failed because the local node is not participating in the network.	Messages could not be sent because the DeviceNet Unit is OFFLINE.
--	--	00: Request 80: Response + Bit 7: ON Bits 0 to 6: Command origin node address			Consider the following items. • Are baud rates for the Standard Master and Standard Slaves on the network the same? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise?
					The message will be discarded and operation continued.
--	--	0106	Temporary	Transmission failed because of a node address duplication error.	Messages could not be sent because a node address duplication error occurred.
--	--	00: Request 80: Response + Bit 7: ON Bits 0 to 6: Command origin node address			Check the node addresses of the other devices. Make sure that the same address is not set for two node and restart the DeviceNet Unit.
					The message will be discarded and operation continued.
--	--	0107	Temporary	Transmission failed because the other node is not participating in the network.	Connection to the destination device was cutoff and a response to the message could not be sent.
--	--	00: Request 80: Response + Bit 7: ON Bits 0 to 6: Command origin node address			Consider the following items. • Is the power supply to the destination device OFF? • Are the baud rates for devices on the network may the same? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise?
					The message will be discarded and operation continued. (When a response is sent, an error response will be returned.)
--	--	0109	Temporary	Transmission failed because the other node is busy.	When a message was sent, the destination device returned a notification that there is no buffer.
--	--	00: Request 80: Response + Bit 7: ON Bits 0 to 6: Command origin node address			Reduce the load on the communications Target.
					The message will be discarded and operation continued.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
--	--	010B	Temporary	Transmission failed because of a CPU Unit error.	The message could not be sent because there was an error with the NE2A-series CPU Unit.
--	--	00: Request. 80: Response + Bit 7: ON Bits 0 to 6: Command origin node address			Consider the following item. • Is there a lot of noise?
					The message will be discarded and operation continued.
--	--	0111	Temporary	Transmission failed because the command exceeded the max. command length.	The command exceeded the maximum data size (522 bytes) as the message response.
--	--	00: Request 80: Response + Bit 7: ON Bits 0 to 6: Command origin node address			Reduce the read size of the communications Target request.
					The message will be discarded and operation continued.
--	--	0112	Temporary	Transmission failed because of a header error.	A connection timeout was detected and the connection was cutoff when trying to send a message response.
--	--	00: Request 80: Response + Bit 7: ON Bits 0 to 6: Command origin node address			Reconsider the following items. • Is the communications Target power supply OFF? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise?
					The response message will be discarded and operation continued.
--	--	0348	Temporary	Message discarded because a new request was received.	A new request was received while a message response was being sent. Transmission of the response was canceled.
--	--	00: Request 80: Response + Bit 7:ON Bits 0 to 6: Command origin node address			Check the transmission interval for requests from the communications Target.
					The response message will be discarded and operation continued.
--	--	--	--	Received data size exceeded limit.	The receivable data size (552 bytes) was exceeded by an Explicit Message Request.
--	--	--			Check the size of the message at the source device and reduce the message size of the request.
					Received data will be discarded and operation continued.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indi-cators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
--	--	--	--	Internal receiver buffer full.	The message request was received but the internal buffer could not be obtained.
--	--	--			Reduce the message request load sent to the DeviceNet Unit.
					Received data will be discarded and operation continued.

19-4 Troubleshooting EtherNet/IP Unit Errors

19-4-1 Checking the EtherNet/IP Unit Error Status

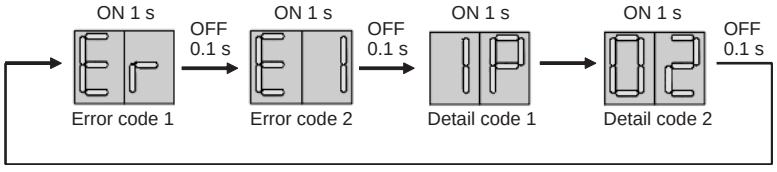
Status Indicator

The status indicators show the status and error codes of an EtherNet/IP Unit. Refer to *3-7-2 Indications*.

Seven-Segment Display

The 2-digit 7-segment display shows the status and error codes of an EtherNet/IP Unit. Refer to *3-7-2 Indications*.

The error code and detail code are displayed alternately.



Error Code

Error code 2 displayed on the 7-segment display generally indicates the following error categories.

Error code	Error category
OFF	Errors related to the EtherNet/IP Unit.
A*	Errors related to the Safety I/O Communications.
C*	Errors with switch operation.
d*	Errors related to the Master.
E*, F*	Errors related to the network.
H*	Errors related to interaction with the CPU Unit.
L*.	Errors related to the Tag Data Link (Target) function.
--	Errors related to message communications.

19-4-2 EtherNet/IP Unit Error Status and Countermeasure

Interpreting the Error Status and Countermeasures

The following table describes the abbreviations that appear in the tables of error codes.

Item			Description
Communications Unit (EtherNet/IP Unit)	Indicators	MS NS	Gives the status of the MS and NS indicators. Top row: MS indicator --: No change in display. Bottom row: NS indicator --: No change in display.
	7-segment display	Error Detail	Gives the error code and detail code displayed on the 7-segment display. Error code 1 (Er) displayed on the 7-segment display is a code that indicates an error. It is not given in this section. Top row: Error code 2 Gives the lower 2-digits of the error code. Middle row: Detail code 1 Gives the upper 2-digits of the error code. IP: IP address bP: BOOTP server address dn: Node address on DeviceNet Bottom row: Detail code 2 Gives the lower 2-digits of the detail code. Gives the address distinguished by detail code 1.
Network Configurator	Error History	Error Detail	Gives the error and detailed information recorded in the error history table. (Information displayed in the Error History Monitor Dialog Box.) Top row: Error code ----: Not saved in error history. (Not saved in error history table.) Bottom row: Detail code ----: Not saved in error history. (Not saved in error history table.)
		Saved	Indicates whether a record is saved in the error history. No: No record is saved in the error history. Temporary: A record is saved in the error history, but it is deleted when the Unit power is turned OFF. Yes: A record is saved in the error history, and it is not deleted when the Unit power is turned OFF.
	Displayed message		Gives the message displayed in the Safety Connections Monitor Dialog Box.
Error name			Names are used to identify errors. Error names are not displayed in the Error History Monitor Dialog Box of the Network Configurator.
Cause Recovery method Status after error			Top row: Cause Gives the cause of the error. Middle row: Reset Gives the method of resetting the error. Bottom row: Status after error Gives the status of the NE2A-series Controller after the error has occurred.

System Errors Related to the EtherNet/IP Unit

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
Lit red OFF	OFF	0601 ****	Yes	Special Unit Error.	An EtherNet/IP Unit hardware error has occurred. Replace the EtherNet/IP Unit if the error recurs when the Controller is restarted. Operation stops.

Communications Unit		Error name	Cause Recovery method Status after error
Indicators	7-segment display		
MS NS	Error Detail		
Lit red OFF	OFF	Special Unit Error.	An EtherNet/IP Unit hardware error has occurred. Replace the EtherNet/IP Unit if the error recurs when the Controller is restarted. Operation stops.
Lit red OFF	H3 IP Local node address	Special Unit Error.	An EtherNet/IP Unit hardware error has occurred. Replace the EtherNet/IP Unit if the error recurs when the Controller is restarted. Operation stops.

CPU Errors for EtherNet/IP Units

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
Flashing red OFF	F4 IP Local node address	020F 0001	Yes	Communications Controller Error.	An EtherNet/IP Unit hardware error has occurred. Replace the EtherNet/IP Unit if the error recurs when the Controller is restarted. • The Unit goes offline and communications will be disabled. An error will be returned for all communications requests. • Data exchange (refresh process) with the CPU Unit will be continued.
Flashing red OFF	H6 IP Local node address	000F 0000	Yes	CPU Unit faulty.	A communications error occurred between the EtherNet/IP Unit and CPU Unit. Replace the CPU Unit if the error recurs when the Controller is restarted. Operation stops.
Flashing red OFF	Hb IP Local node address	0011 No display	Yes	CPU Unit event servicing timeout.	A timeout occurred while reading parameters to the CPU Unit. Replace the EtherNet/IP Unit and/or the CPU Unit if the error recurs when the Controller is restarted. Operation stops.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
Flashing red OFF	F4 IP Local node address	020F 0001	Yes	Communications Controller Error.	An EtherNet/IP Unit hardware error has occurred. Replace the EtherNet/IP Unit if the error recurs when the Controller is restarted. • The Unit goes offline and communications will be disabled. An error will be returned for all communications requests. • Data exchange (refresh process) with the CPU Unit will be continued.

Communications Unit		Error name	Cause Recovery method Status after error
Indicators	7-segment display		
MS NS	Error Detail		
Flashing red OFF	H0 IP Local node address	CPU Unit Connection error with unsupported device.	The EtherNet/IP Unit is connected to a CPU Unit that does not support it. Check the CPU Unit. Mount the EtherNet/IP Unit properly. Operation stops.
Flashing red OFF	H1 IP ---	Unit number setting error.	The unit number is duplicated or is invalid. An EC.13 error may occur in the CPU Unit. Correct the unit number setting and restart the EtherNet/IP Unit. Operation stops Monitoring is not possible with the Network Configurator.
Flashing red OFF	H2 IP Local node address	Unit Identification Error.	A Unit identification error has occurred at the CPU Unit. Replace the CPU Unit if the error recurs when the Controller is restarted. Operation stops.

Hardware Setting Errors for EtherNet/IP Units

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
Flashing red Lit red	F0 IP Local node address	0211 02 + IP address	Yes	IP Address Duplication.	The same EtherNet/IP Unit IP address is set for another node. Check the IP addresses of other nodes. Change the settings so that there are no duplications and restart the EtherNet/IP Unit. • The Unit will be offline and communications disabled. An error will be returned for all communications requests. • Data exchange with the CPU Unit (refresh) will be continued.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
Flashing red --	C8 IP Local node address	03D9 Refer to *Cause* column.	Yes	Switch changed during operation.	**(1)** The IP address setting switches were changed during operation. Error detail: 02 + Value before switch was changed **(2)** After the configuration was completed, the IP address was changed by the IP address rotary switches or a software setting, and operation was restarted. Error detail: 03 + Rightmost byte of IP address when configuration is completed
					Reset the setting to what it was before the change was made. Alternatively, restart the EtherNet/IP Unit after the change is made. Download the IP address configuration data that matches the IP address set by the BOOTP, TCP/IP setting, or node address setting switch.
					Safety I/O Communications will be stopped. Tag Data Links (Standard I/O Communications) and other operations will be continued. Safety I/O Communications will be restarted if the switch setting is reset to its original setting.
Flashing red --	E8 IP Local node address	021A 000E	Yes	Logic error in configuration data.	A recoverable parameter error occurred in the Network Configurator.
					Check the device parameter. Normal operation will resume when the Network Configurator has completed writing the parameters.
					Operates with default settings.
Flashing red --	E9 IP Local node address	0602 No display	Yes	Memory access error.	An error occurred when reading/writing to the non-volatile memory in the Unit. A record may not be saved in the error history in some cases.
					If the error recurs after restarting, replace the EtherNet/IP Unit.
					Non-volatile memory writing is ignored and operation continues.
Flashing red --	F2 IP Local node address	03D0 No display	Yes	Ethernet Basic Settings Error.	A checksum error or a logic error occurred in the basic EtherNet settings.
					Download the TCP/IP settings from the Network Configurator.
					Operation will be continued by setting the basic Ethernet settings where the error occurred to default values. However, Safety I/O Communications and Standard I/O Communications will be stopped.
Flashing red --	H9 IP Local node address	000E 0000	Yes	I/O bus error.	An error occurred when data was exchanged with the CPU Unit.
					Review the operating environment of the CPU Unit.
					Safety I/O Communications will be stopped. The output data of the Tag Data Link's Target connection will continue sending refreshed data. If the CPU Unit status is set, the CPU Unit error will be ON.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
Flashing red --	HC IP Local node address	021A 000E	Yes	Routing table logic error.	There is an error with the CPU Unit configuration data. An EC.12 error may occur in the CPU Unit. If the error recurs after restarting, replace the EtherNet/IP Unit or the CPU Unit. Operation stops.
Flashing red --	HE IP Local node address	0002 No display	Yes	CPU Unit service monitoring error.	Service from the CPU Unit is disabled for a period. Monitoring is normally for 11 s. Review the CPU Unit operation environment. Replace the CPU Unit if the error recurs. Safety I/O Communications will be stopped. The output data of the Tag Data Link's Target connection will continue sending refreshed data. If the CPU Unit status is set, the CPU Unit error will be ON. The message will be discarded if the received message needs to be passed to the CPU Unit. Returns to normal operation when the error is reset.
Flashing red --	HF IP Local node address	0001 0000	Yes	CPU Unit watchdog timer error.	An error occurred in the CPU Unit. Review the CPU Unit's operation environment. Replace the CPU Unit if the error recurs. Safety I/O communications will stop. Tag Data Link Target connection output data will stop being sent. If the CPU Unit status is set, a CPU Unit error will occur. The message will be discarded if the received message needs to be passed to the CPU Unit.

Communications Errors for EtherNet/IP Units

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
-- --	E1 IP Local node address	03D3 0000	Temporary	Ethernet Link Not Detected.	The link between switching hubs cannot be detected. Consider the following items. • Is the cable connected? • Is the Hub power supply ON? • Are any cables disconnected or loose? • Is there a lot of noise? The Unit will go offline and communication will be disabled. An error will be returned for all communications requests. Data exchange with the CPU Unit (refresh) will be continued.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
-- Flashing red	A1 IP Local node address	2100 00 + IP address	Yes	Part of the System stopped due to Safety I/O Communications error.	The Safety Master connection supported by the EtherNet/IP Unit was disconnected while part of the System was stopped due to a Safety I/O Communications error.
					Establish communications again from the Network Configurator.
					The Safety I/O Connection where the error occurred will remain stopped without establishing the connection again. Any other operations will be continued.
-- Flashing red	d5 IP Target node address	2101 2C + IP address	Yes	Nonexistent Safety Slave Device.	No Standard Slave devices exist in the network when the Standard Master connection is being established.
					Consider the following items. • Is the Safety Slave power supply OFF? • Is the Safety Slave IP address correct? • Is the cable connected? • Are any cables disconnected or loose? • Is there a lot of noise?
					The recovery method depends on the setting for when an error occurs in Safety Communications. • Connection Stop Mode The Safety I/O Connection where the error occurred will be stopped. • Automatic Recovery Mode Repeated attempts will be made to establish the Safety I/O Connection again. All other operations will be continued.
-- Flashing red	d6 IP Target node address	2101 1st byte: No display 2nd byte: IP address	Yes	Nonexistent Safety Slave Device.	The Safety Slave device configuration information is invalid or Safety I/O Communications is disabled when the Safety Master connection is being established.
					Consider the following items. • Is the Safety Slave IP address correct? • Is the Safety Slave configuration correct? • Is the Safety Slave operating mode correct?
					The recovery method depends on the setting for when an error occurs in Safety Communications. • Connection Stop Mode The Safety I/O Connection where the error occurred will be stopped. • Automatic Recovery Mode Repeated attempts will be made to establish the Safety I/O Connection again. All other operations will be continued.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
-- Flashing red	dA IP Target node address	2102 01 + IP address	Yes	Safety I/O Connection Timeout.	A communications timeout occurred during Safety I/O Communications with a Slave.
					Consider the following items. • Is the Safety Slave IP address correct? • Is the Safety Slave configuration correct?
					The recovery method depends on the setting for when an error occurs in Safety Communications. • Connection Stop Mode The Safety I/O Connection where the error occurred will be stopped. • Automatic Recovery Mode Repeated attempts will be made to establish the Safety I/O Connection again. All other operations will be continued.
-- Flashing red	L9 IP Target node address	03D5 02 + IP address	Yes	Tag Data Link Error.	A timeout occurred during Tag Data Link communications by the Target function.
					Consider the following items. • Is the Originator operating properly? • Is the cable connected? • Are any cables disconnected or loose? • Is there a lot of noise?
					An error will be returned for any requests for communications to the Originator with the error. The communications will be restarted by establishing the connection from the Originator again.
-- Flashing Red	LA IP Target node address	2102 01 + IP address	Yes	Safety I/O Connection Timeout.	A communications timeout occurred during Safety I/O Communications with the Master.
					Consider the following items. • Is the Safety Slave IP address correct? • Is the Safety Slave configuration correct?
					The recovery method depends on the setting for when an error occurs in Safety Communications. • Connection Stop Mode The Safety I/O Connection where the error occurred will be stopped. • Automatic Recovery Mode Repeated attempts will be made to establish the Safety I/O Connection again. All other operations will be continued.

Communications Unit		Network Configurator			Cause Recovery method Status after error
Indicators	7-segment display	Error history		Displayed message	
MS NS	Error Detail	Error Detail	Saved		
-- --	E3 IP	03C4 0001	Temporary	Server Connection Error.	An error occurred between the BOOTP Server and the EtherNet/IP Unit. 1) There is no response from the BOOTP server. 2) The IP address set to the EtherNet/IP Unit from the BOOTP server was invalid.
					Check the status and settings of the BOOTP server.
					Requests to the BOOTP server will continue until there is a response. If the address received from the BOOTP server is invalid, the IP address will be discarded. In the mean time, the Unit will go offline and communications will be disabled. An error will be returned for all communications requests. Data exchange with the CPU Unit (refresh) will be continued.
--	-- --	0118	Temporary	Invalid message discarded.	An unexpected frame was received and therefore discarded.
--	--	FFFF			Check Target device messages.
					Operation continues.

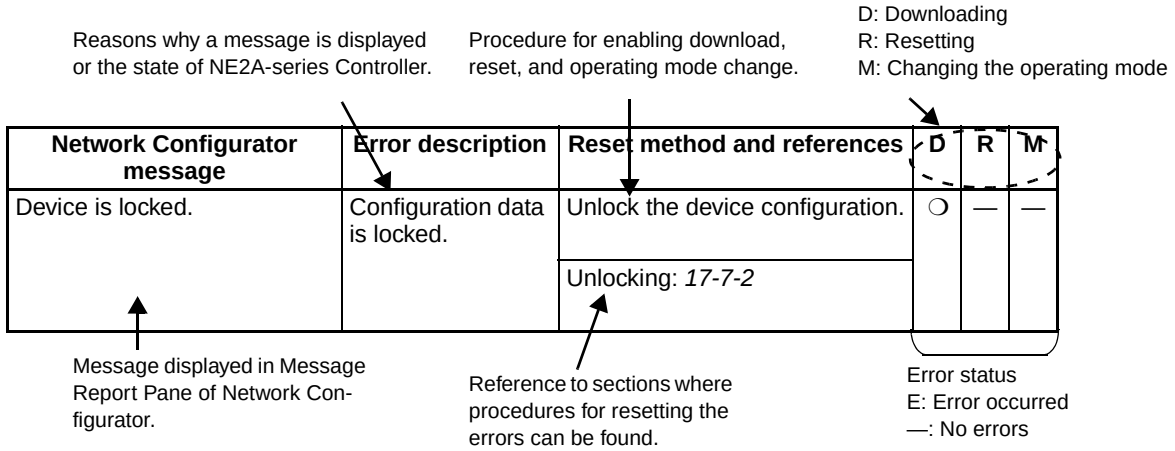
19-5 Troubleshooting Network Configurator Errors

19-5-1 Checking the Network Configurator Error Status

Errors can occur when configuration data is downloaded to the NE2A-series Controller, reset, or the operating mode is changed. The causes of the errors are determined according to the display in the Message Report Pane in the Network Configurator.

19-5-2 Network Configurator Errors and Countermeasures

Interpreting the Error Status and Countermeasures



Error Table

Network Configurator message	Error description	Reset and Relevant sections	D	R	M
Privilege violation.	You cannot change or reset the configuration, nor change the operating mode with the password you are using.	Check whether the password you are using is correct. Connecting through a USB: *17-2-1* Downloading: *17-3-1*	E	E	E
Cannot be executed in the current device mode.	Data is being downloaded simultaneously from multiple Network Configurators.	Wait until the other downloads have been completed.	E	—	—
Cannot be executed in the current mode	An abort fatal error has occurred. (The MS Indicator is flashing red.)	Correct the switch setting or reset to default setting to clear the configuration data. If an error occurs when the operating mode is changed, download the device parameters again. Switches: *3-2-3* Resetting: *17-8-1* Downloading: *17-3-1*	E	—	E
	The configuration cannot be reset with the NE2A-series Controller in the current status.	Refer to *17-8-2 Reset Types and Device Status* to change the configuration lock status of the NE2A-series Controller. Locking: *17-7-2*	—	E	—
	The device is not configured.	Download the device parameters. Downloading: *17-3-1*	—	—	E
Connection failed.	Connection could not be established when attempting to configure a device on the DeviceNet network through the USB on the NE2A-series Controller.	Check that power is supplied to the device and download the data again. In situations other than that described in the error description, communications may be unstable because of noise. Check the following items. • Are baud rates of all nodes the same? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line? • Is there a lot of noise? Downloading: *17-3-1*	E	E	E
Could not open connection.	The Network Configurator could not connect to the NE2A-series Controller while downloading through the DeviceNet or the Ethernet.	Check that power is supplied to the device and try again.	E	—	—
	A connection to the Network Configurator cannot be established because the device is using all available connections to conduct Safety I/O Connections with the Safety Master.	Change the operating mode of the Safety Master registered with a Safety Connection to IDLE Mode. Operating mode change: *17-5-1*	E	—	—
	In situations other than that described above, communications may be unstable because of noise.	Check the following items. • Are the baud rates of all nodes the same? • Are the cable lengths (branch/main lines) suitable? • Are any cables disconnected or loose? • Is there a terminator at each end of the main line?	E	—	—
Already set to the specified operating mode.	The device is already set to specified mode.	--	—	—	E

Network Configurator message	Error description	Reset and Relevant sections	D	R	M
The device is locked.	Configuration data is locked. (LOCK indicator is lit.)	Unlock the configuration. Locking: *17-7-2*	E	—	—
The device cannot be accessed or the device type or password is different.	The device is in a state immediately after being reset or the power supply was switched OFF and ON. Communications is not enabled. (Online status or NS indicator is flashing green or lit red.)	Check that communications is enabled for the device, and then begin the communication. Device status: *9-6-2*	—	E	E
	The device may not support services when an operating mode change is requested.	Check that the device node address is correct. Node address: *9-6-2*	—	E	E
	Configuration data is locked. (LOCK indicator is lit.)	Unlock the configuration. Unlocking: *17-7-3*	—	E	—
	The configuration cannot be reset because the NE2A-series Controller is conducting Safety I/O Communications.	Change the operating mode of the relevant Safety Master to IDLE Mode. Operating mode change: *17-5-1*	—	E	—
Could not access the device.	The NE2A-series Controller was reset from another node while downloading. It is waiting for the TUNID. (NS indicator is flashing green/red.)	Set the network number and download the data again. Network number: *11-3-1*, *12-3-1* Downloading: *17-3-1*	E	—	—
The device has a different TUNID.	A device was reset and is waiting for the TUNID to be set. (MS indicator flashing green/red.) Alternatively, the TUNID of the device is different from the TUNID specified by the Network Configurator.	Check the setting with the following procedure. 1. Downloading (1) Start downloading again after resetting the device to default setting. However, the network number may not match with other devices. After changing the NE2A-SCPU01 to RUN mode, if bit 6 is displayed on the 7-segment display (“Safety I/O Connection Establishment Failure” displayed in error history), do the following step. (2) Execute uploading from the network and reset all devices to the default settings. Download the data to all the devices again after resetting the configuration. 2. Changing the Operating Mode Check whether the device node address matches. If it does, the network number of the device and Network Configurator do not match. Upload from the network using the Network Configurator so that the network number matches. Resetting: *17-8-1* Downloading: *17-3-1* Uploading: *17-3-2* Network number: *11-3-1*, *12-3-1*	E	—	E
The device has a different TUNID.The device TUNID will be used to reset. Is that OK?	The TUNID of the device is different from the TUNID specified by the Network Configurator.	Check that the node address is correct for the device. The configuration will be reset with the device TUNID if there is no problem. Node address: *9-6-2*	—	E	—

Network Configurator message	Error description	Reset and Relevant sections	D	R	M
An error was found during parameter check.	Configuration parameters are not consistent.	Check the following items and modify the parameters. • Timing parameters such as discrepancy time set for the I/O Unit are smaller than the cycle time in the NE2A-series Controller. • The Safety Connection EPI is smaller than the cycle time. • The Safety I/O configuration is set so that the connection ID of the Safety Master exceeds the maximum number (12). Set the Safety Connection to Confirm Produced IDs to Safety Slaves. Cycle time: *10-2-1* EPI setting: *13-2-1* Safety Connections: *11-4-2*	E	—	—
	The hardware may be faulty.	Switch the NE2A-series Controller power supply from OFF to ON and execute self-diagnosis. Replace the CPU Unit if the MS indicator is lit red.	E	—	—
Program incomplete. Start Logic Editor and check program.	There is an input or output that is not connected in the function block used in the program.	Open the Logic Editor and do one of the following. • Connect the disconnected input or output. • Delete the disconnected input or output by modifying the Input and Output Size Setting of the function block. The function block with the disconnected input or output can be checked using the build function. Connecting: *15-6-6* Input and Output Size Setting: *15-6-3* Build: *15-8-1*	E	—	—
Message could not be sent.	The Network Configurator could not connect to the NE2A-series Controller when data was downloaded through a USB connection.	Check that power is supplied to the device and send the message again.	E	—	—
The data used by the user program is not aligned with other data.	Data used by the logic program does not align with other data because the network configuration was changed.	Start the Logic Editor and check where the inputs and outputs were changed. Download the data. Starting the Logic Editor: *15-3-1* Downloading: *17-3-1*	E	—	—

19-6 Connection Status Tables

19-6-1 Outline

If an error occurs when the NE2A-series Controller tries to establish a safety connection with a DST1/NE0A-series Safety I/O Terminal or an NE1A/NE2A-series Controller set as a Slave, the 7-segment display will display the error code “d6” or “d5.” If an error occurs during I/O communications, the 7-segment display will display the error code “dA.”

For an EtherNet/IP Unit, "IP" (for the IP address) or "dn" (for a DeviceNet node address) will be displayed next, followed by the address of the Safety Slave in hexadecimal (i.e., the lower two bytes of the IP address).

Check the status code (error code) shown on the Safety Connection Tab Page in the Monitor Device Window and take the corresponding countermeasure.

19-6-2 Connection Status for DST1/NE0A Series

Status		Countermeasure
00:0001*	Normal communications	The Safety I/O connection status is normal. A number between 1 and F (hexadecimal) will be displayed for *. The number of Safety Masters that are communicating on the same multicast connection will be shown.
01:0001	Safety I/O Connection Timeout	The Safety I/O connection has timed out. Check the following items. • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise? • Is the network bandwidth allocation suitable?
01:0105	Configuration Owner Error	The Safety Slave was configurated from a configuration tool or Safety Master at a different node address last time. Reset the Safety Slave to the default settings and download the device parameters again.
01:0106	Output connection Owner Error	The Safety Slave established output safety I/O connections with a Safety Master at a different node address last time. Reset the Safety Slave to the default settings and download the device parameters again.
01:0110	Device Not Configurated	The Safety Slave has not been configurated. Download the device parameters to the Safety Slave.
01:0113	No. of Connections Error	The setting for the number of safety I/O connections exceeds the upper limit supported by the Safety Slave. Adjust the Safety Connection setting for the relevant Safety Master.
01:0114	Vendor ID or Program Code Error	The device data (vendor ID or product code) for the device on the Configurator and the device used in the actual system does not match. • Use Safety Slave Verification (***Device*** – ***Parameter*** – ***Verify***) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.
01:0115	Device Type Error	The device data (device type) for the device on the Configurator and the device used in the actual system does not match. • Use Safety Slave Verification (***Device*** – ***Parameter*** – ***Verify***) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.
01:0116	Revision Error	The device data (revision) for the device on the Configurator and the device used in the actual system does not match. • Use Safety Slave Verification (***Device*** – ***Parameter*** – ***Verify***) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.

Status		Countermeasure
01:0117	Connection Path Error	1. Two or more output safety I/O connections have been set for the Safety Slave. • Change the Safety Connection setting for the Safety Master so there is only one connection. Then reset the Safety Slave to default settings and download the device parameters to the Safety Slave again. 2. The same output assembly number for a Safety Slave has been used for both a Safety Master and a Standard Master. • Input assembly numbers can be duplicated but output assembly numbers cannot. Check the Safety Connection setting for both the Safety Master and the Standard Master then return the Safety Slave to default settings and download the device parameters to the Safety Slave again. • If the error remains even after the above countermeasure has been performed, delete and re-register the connections registered to the Safety Master.
01:0119	Safety I/O Communications Failure	The execution mode of the DST1-XD□□ Safety Slave was set to Auto Execution. Safety I/O communications are not possible in Auto Execution Mode. If the DST1-XD□□ Safety Slave is to be used with safety I/O communications, set the execution mode to *After Establishing Safety I/O Connection.*
01:031E	No. of Connections Error	The setting for the number of safety I/O connections exceeds the upper limit supported by the Safety Slave. Adjust the Safety Connection setting for the relevant Safety Master. In particular, check that no more than 15 Safety Masters are set for each Multicast connection, with a maximum total of 30. When setting connections from an EtherNet/IP Unit through an NE1A-EDR01 ED Router, make sure that no more than 32 connections have been set for one ED Router. (Each multicast connection is counted as two connections.)
01:031F	Connection ID Resource Error	The maximum number of connection IDs for one Safety Master (12) has been exceeded. Check the Safety Connection settings of the relevant Safety Master.
01:07FF	Non-existent Safety Slave	The Safety Slave may not have been added to the network correctly. Check that the corresponding Safety Slave is online (i.e., the NS indicator is flashing green or lit green.) If the Safety Slave is not online, check the following items. • Is the node address for the Safety Slave correct? • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise?
01:080C	Safety Signature Mismatch	The safety signature for the Safety Slave monitored by the Safety Master does not match the safety signature of the Safety Slave itself. • Reset the Safety Slave to default settings then download the device parameters again. • If the above remedy does not work, delete then re-register the connections registered to the Safety Master.
01:080E	TUNID Mismatch	The TUNID for the Safety Slave monitored by the Safety Master does not match the TUNID of the Safety Slave itself. • Reset the Safety Slave to default settings then download the correct device parameters. • If the above remedy does not work, delete then re-register the connections registered to the Safety Master.

Status		Countermeasure
01:080F	Safety Configuration not possible	1. The Safety Slave is configuration locked and *Configure the target device* is selected for the Open Type setting for the Safety Master connection. • Release the configuration lock on the Safety Slave to configure the Safety Slave from the Safety Master. • To configure the Safety Slave from a configuration tool, set the Safety Master connection to *Check the safety signature* under Open Type. Then reset the Safety Slave to default settings and download the device parameters to the Safety Slave again. 2. The execution mode of the DST1-XD□□ Safety Slave was set to Auto Execution and then the open type setting in the safety connection settings in the safety master was set to configure a safety slave. • Safety I/O communications are not possible in Auto Execution Mode. If the DST1-XD□□ Safety Slave is to be used with safety I/O communications, set the execution mode to After Establishing Safety I/O Connection.
0C:0002	Communications Partner in IDLE Mode	The NE0A-series Controller that is being communicated with is in IDLE Mode, making it impossible to establish a Safety I/O Connection. Change the operating mode of the NE0A-series Controller that is functioning as the Safety Slave to RUN Mode.
D0:0001	IDLE Mode	Safety I/O communications have not been started because the NE2A-series CPU Unit that is the safety master is in IDLE Mode. Change the NE2A-series CPU Unit to RUN mode.

19-6-3 Connection Status for the NE1A-series Controller (Safety Slave Function)

Status		Countermeasures
00:0001*	Normal communications	The Safety I/O connection status is normal. A number between 1 and F (hexadecimal) will be displayed for *. The number of Safety Masters that are communicating on the same multicast connection will be shown.
01:0001	Safety I/O Connection Timeout	The Safety I/O connection has timed out. Check the following items. • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise? • Is the network bandwidth allocation suitable?
01:0106	Output Connection Owner Error	The Safety Slave has previously established an output safety I/O connection with a Safety Master at a different node address. Reset the Safety Slave to the default settings, and then download the device parameters again.
01:0109	Data Size Error	The Safety Slave I/O size set to the NE1A/NE2A-series Safety Slave and the size set under the Safety Master safety connection setting does not match. The Safety Slave I/O setting may have been changed, so delete then re-register the connections registered to the Safety Master.
01:0110	Unconfigured Device	The Safety Slave has not been configurated. Download the device parameters to the Safety Slave.
01:0111	EPI Error	The EPI set under the Safety Master safety connection setting is smaller than the Safety Slave cycle time. The EPI must be longer than both the Safety Master and the Safety Slave cycle times. Check the Safety Master safety connection setting.
01:0113	No. of Connections Error	The setting exceeds the maximum number of safety I/O connections supported by the Safety Slave. Check the relevant Safety Master safety connection settings.
01:0114	Vendor ID or Product Code Error	The device data (vendor ID or product code) for the device on the Configurator and the device used in the actual system does not match. • Use Safety Slave Verification (***Device*** – ***Parameter*** – ***Verify***) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.
01:0115	Device Type Error	The device data (device type) for the device on the Configurator and the device used in the actual system does not match. • Use Safety Slave Verification (***Device*** – ***Parameter*** – ***Verify***) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.
01:0116	Revision Error	The device data (revision) for the device on the Configurator and the device used in the actual system does not match. • Use Safety Slave Verification (***Device*** – ***Parameter*** – ***Verify***) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.

Status		Countermeasures
01:0117	Connection Path Error	Two ore more single-cast safety I/O connections or a multicast safety I/O connection with a different EPI has been set for a safety slave I/O. • To share one safety slave I/O on a Safety Slave with more than one Safety Master, make the EPI all the same and set the connection type to Multicast. • NE1A-series Safety Slaves cannot have more than one single-cast safety I/O connection for each Safety Slave I/O. Set multiple connection paths for the NE1A-series Safety Slave Safety Slave I/O. • If the connection is not restored with the above remedy, delete then re-register the connections registered to the Safety Master.
01:031E	No. of Connections Error	The setting for the number of safety I/O connections exceeds the upper limit supported by the Safety Slave. Adjust the Safety Connection setting for the relevant Safety Master. In particular, check that no more than 15 Safety Masters are set for each Multicast connection, with a maximum total of 60. When setting connections from an EtherNet/IP Unit through an NE1A-EDR01 ED Router, make sure that no more than 32 connections have been set for one ED Router. (Each multicast connection is counted as two connections.)
01:031F	Connection ID Resource Error	The maximum number of connection IDs for one Safety Master (12) has been exceeded. Check the Safety Connection settings of the relevant Safety Master.
01:07FF	Non-existent Safety Slave	The Safety Slave may not have been added to the network correctly. Check that the corresponding Safety Slave is online (i.e., the NS indicator is flashing green or lit green.) If the Safety Slave is not online, check the following items. • Is the node address for the Safety Slave correct? • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise?
01:080C	Safety Signature Mismatch	The safety signature for the Safety Slave monitored by the Safety Master does not match the safety signature of the Safety Slave itself. • Reset the Safety Slave to default settings then download the device parameters again. • If the above remedy does not work, delete then re-register the connections registered to the Safety Master.
01:080E	TUNID Mismatch	The TUNID for the Safety Slave monitored by the Safety Master does not match the TUNID of the Safety Slave itself. • Reset the Safety Slave to default settings then download the correct device parameters. • If the above remedy does not work, delete then re-register the connections registered to the Safety Master.
D0:0002	Safety slave that is communications partner is in IDLE Mode	The communications partner, a NE1A/NE2A-series Controller that is functioning as a safety slave, is in IDLE Mode, so a safety I/O connection cannot be established. Change the operating mode of the communications partner to RUN Mode.
10:0001	I/O communications have stopped at Safety Slave that is the communications partner	Safety I/O connections cannot be established because I/O communications have stopped at NE2A-series Controller that is functioning as the Safety Slave that is the communications partner. Start I/O communications at the NE2A-series Controller that is functioning as the Safety Slave.
D0:0001	IDLE Mode	The NE2A-series CPU Unit that is functioning as the safety master is in IDLE mode, so a safety I/O communications have not been started. Change the NE2A-series CPU Unit's operating mode to RUN mode.

SECTION 20
Inspections and Maintenance

This section describes the inspections and maintenance that are required to ensure proper operation of a NE2A-series Safety Network Controller system.

20-1 Inspections 542
20-2 NE2A-series Unit Replacement Precautions 543

20-1 Inspections

Daily or periodic inspections are required in order to maintain the NE2A-series Controller functions in peak operating condition.

- Confirm that the NE2A-series Controller is being used within the specifications.
- Confirm that the NE2A-series Controller is mounted and wired correctly.
- Check the safety functions in order to maintain their operating reliability at a constant level.
- Use the error log to check for non-fatal errors.

Periodic Inspection Points

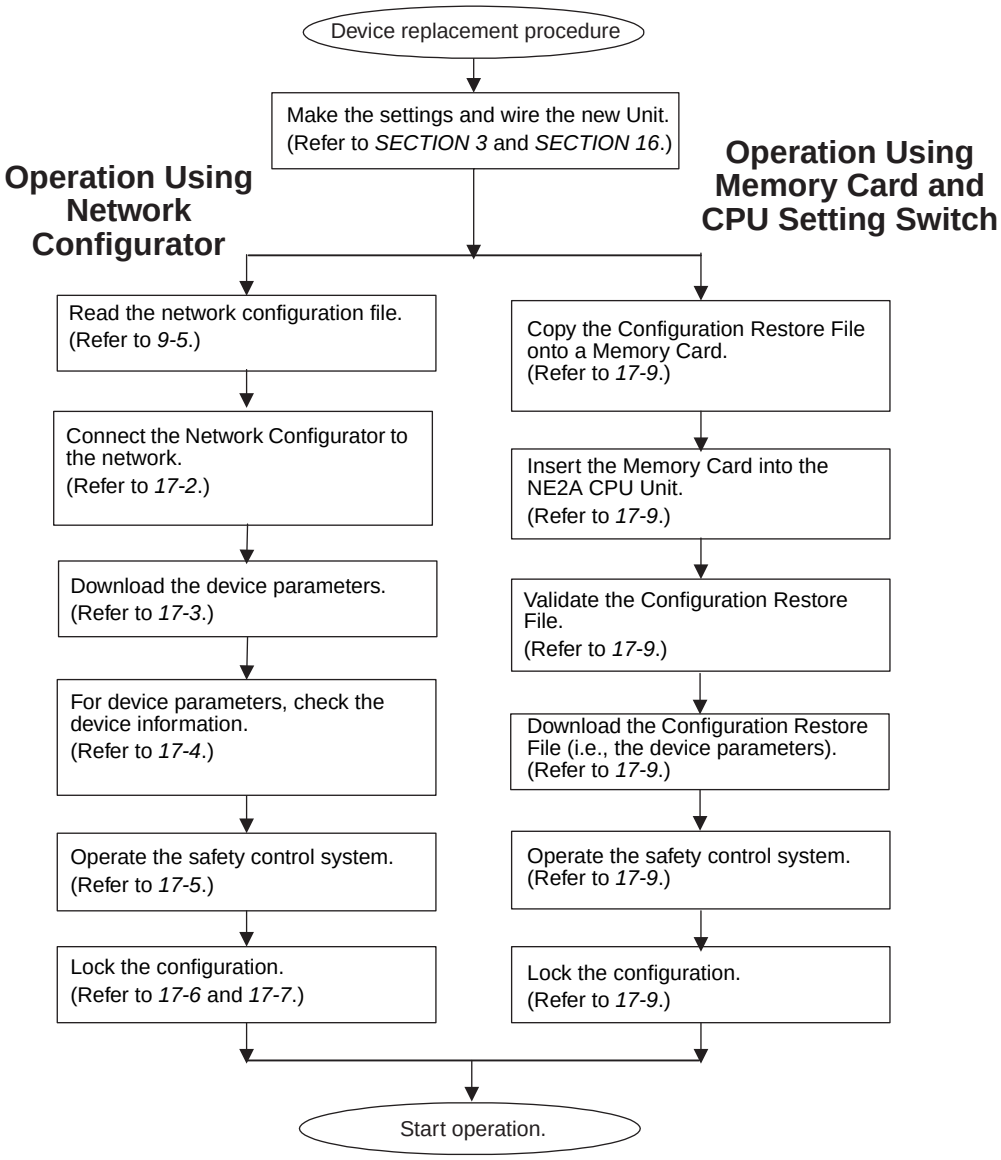
No.	Item	Inspection	Criteria	Action
1	Source power supply	Check for voltage fluctuations at the power supply terminals.	The voltage must be within the allowable voltage fluctuation range. (Refer to *SECTION 3*.)	Use a voltage tester to check the power supply at the terminals. Take necessary steps to bring voltage fluctuations within limits.
2	I/O power supply	Check for voltage fluctuations at the I/O terminals.	Voltages must be within specifications for each Unit. (Refer to *3-8* and *3-9*.)	Use a voltage tester to check the power supply at the terminals. Take necessary steps to bring voltage fluctuations within limits.
3	Ambient environment	Check the ambient temperature. (Inside the control panel if the Controller is in a control panel.)	0 to 55°C (Refer to *3-1*.)	Use a thermometer to check the temperature and ensure that the ambient temperature remains within the allowed range of 0 to 55°C.
		Check the ambient humidity. (Inside the control panel if the Controller is in a control panel.)	Humidity must be 10% to 90% with no condensation. (Refer to *3-1*.)	Use a hygrometer to check the humidity and ensure that the ambient humidity remains between 10% and 90%. Make sure that condensation does not occur due to rapid changes in temperature.
		Check that the Controller is not in direct sunlight.	Not in direct sunlight	Protect the Controller if necessary.
		Check for accumulation of dirt, dust, salt, metal filings, etc.	No accumulation	Clean and protect the Controller if necessary.
		Check for water, oil, or chemical sprays hitting the Controller.	No spray on the Controller	Clean and protect the Controller if necessary.
		Check for corrosive or flammable gases in the area of the Controller.	No corrosive or flammable gases	Check by smell or use a sensor.
		Check the level of vibration or shock.	Vibration and shock must be within specifications. (Refer to *3-1*.)	Install cushioning or shock absorbing equipment if necessary.
		Check for noise sources near the Controller.	No significant noise sources (Refer to *3-1*.)	Either separate the Controller and noise source or protect the Controller.
4	Installation and wiring	Check that each Unit is connected and locked to the next Unit securely.	No looseness (Refer to *SECTION 16*.)	Press the connectors together completely and lock them with the sliders.
		Check that cable connectors are fully inserted and locked.	No looseness (Refer to *SECTION 16*.)	Correct any improperly installed connectors.
		Check for loose screws in external wiring.	No looseness	Tighten loose screws with a Phillips screwdriver.

20-2 NE2A-series Unit Replacement Precautions

When replacing an NE2A-series Unit after discovering a problem during inspection, pay attention to the following points.

- Do not attempt to disassemble, repair, or modify the Unit. Doing so may impair the original safety functions.
- Make sure that safety can be assured when replacing the Unit.
- To prevent electric shock or unexpected operation, always turn OFF the power before replacing the Unit.
- After replacing the Unit, check the new Unit to make sure that there are no errors.

Note After replacing an NE2A-series Unit, reset all the settings required for restarting the user program and confirm that the safety functions are operating normally before starting this operation.



Making Settings and Wiring the New Unit

Setting Switches on the New Unit

Referring to *SECTION 3 Configuration Unit Specifications and Nomenclature*, match the switch settings on the new Unit to the settings on the Unit that was replaced.

Replacing and Wiring the Unit

Referring to *SECTION 16 Mounting, Wiring, and Hardware Settings*, remove the faulty Unit and mount and wire the new Unit.

Downloading Parameters and Checking Operation

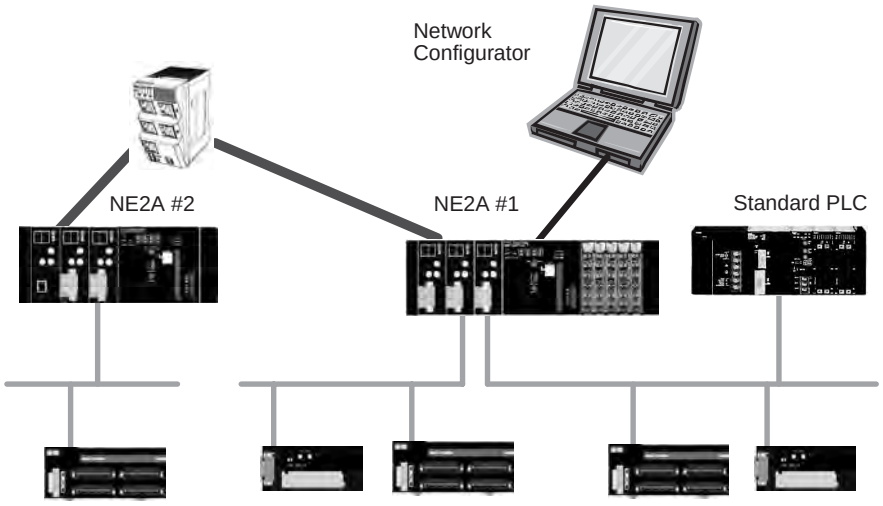
When any Communications Unit or I/O Unit is replaced, the parameters must be downloaded to the NE2A-series CPU Unit to which that Unit is mounted even if the CPU Unit itself has not been replaced.

Operation Using the Network Configurator

Referring to *SECTION 17 Downloading Device Parameters and Operating the Safety Control System*, download the parameters to the NE2A-series Controller to which the new Unit is mounted and check the system operation.

Operation Using a Memory Card and the Setting Switch

Referring to *SECTION 17 Downloading Device Parameters and Operating the Safety Control System*, download the parameters to the NE2A-series Controller to which the new Unit is mounted and check the system operation.



If the NE2A #1 DeviceNet Unit or an I/O Unit is faulty, replace the faulty Unit and download the NE2A #1 parameters. Check the operation of the entire system, including the NE2A #1, NE2A#2, and Standard PLC, and confirm the safety of the system.

Appendix A

Calculated PFD and PFH Values

Calculated PFD and PFH values for the NE2A-series Controller are given in the following tables. You must calculate the PFD and PFH values for all devices in the system to ensure that the SIL required by the application is achieved.

Calculated PFD Values

Model	Proof test interval (years)	PFD
NE2A-SCPU01	0.25	1.14E-06
	0.5	2.27E-06
	1	4.53E-06
	2	9.06E-06
NE2A-SID4-1	0.25	1.86E-07
	0.5	3.71E-07
	1	7.40E-07
	2	1.48E-06
NE2A-SOD4-1	0.25	2.15E-07
	0.5	4.27E-07
	1	8.52E-07
	2	1.70E-06

Calculated PFH Values

Model	PFH
NE2A-SCPU01	1.03E-09
NE2A-SID4-1	1.69E-10
NE2A-SOD4-1	1.94E-10

Note Verify that all safety functions are operating normally in proof testing.

Glossary

The following terms are used with the specified definitions in this manual to describe NE2A-series Network Safety Controllers.

Term	Definition
Communications Unit	The collective name of the NE2A-DNS21 and NE2A-ENS21. These are the DeviceNet Unit and EtherNet/IP Unit that support safety communications.
CPU Unit	The name of the NE2A-SCPU01.
DeviceNet Unit	In this manual, refers to the NE2A-DNS21 DeviceNet Unit for the NE2A. The NE2A-DNS21 DeviceNet Unit supports DeviceNet Safety. The DeviceNet Unit for the OMRON CJ Series is referred to as the CJ DeviceNet Unit or the CJ1W-DRM21.
End Cover	The name of the NE2A-TER01.
End Unit	The name of the NE2A-END.
EtherNet/IP Unit	In this manual, refers to the NE2A-ENS21 EtherNet/IP Unit for the NE2A. The NE2A-ENS21 EtherNet/IP Unit supports EtherNet/IP Safety. The EtherNet/IP Unit for the OMRON CJ Series is referred to as the CJ EtherNet/IP Unit or the CJ1W-EIP21.
EtherNet/IP-DeviceNet Router (ED Router)	The name of the NE1A-EDR01.
I/O Unit	A Unit used to expand the Safety I/O functionality of an NE2A-series Controller a few I/O points at a time. “I/O Unit” is the collective name for the NE2A-SID4-1 and NE2A-SOD4-1.
Network Configurator	The name of the WS02-CFSC-J/E.
Power Supply Unit	The name of the NE2A-PD025.
Remote I/O Terminal	A Remote I/O Terminal for use in Standard controls.
Safety	Refers to devices, functions, or data for which special safety measures for use in safety controls have been implemented.
Safety I/O Terminal	A Remote I/O Terminal for use in safety controls. “Safety I/O Terminal” is the name of the terminals in OMRON's DST1 Series.
Safety Input device	An input device for which special measures for use in safety controls have been implemented. Emergency stop switches and safety door switches are examples of Safety Input devices.
Safety Input Unit	The name of the NE2A-SID4-1.
Safety Network Controller (Controller)	A controller that supports Safety Networks and has a high reliability for use in safety controls. “Safety Network Controller” is the name of the controllers in OMRON's NE0A Series, NE1A Series, and NE2A Series.
Safety Output device	An output device for which special measures for use in safety controls have been implemented. Safety relays are an example of a Safety Output device.
Safety Output Unit	The name of the NE2A-SOD4-1.
Standard	Refers to devices, functions, or data for Standard applications. “Standard” is used to distinguish Standard Devices, functions, or data from those for which special safety measures for use in safety controls have been implemented.
Standard CPU Unit	A CPU Unit for used in Standard Controls. “Standard CPU Unit” is used for the CPU Units in OMRON's CS/CJ Series of PLCs. It is used to distinguish CPU Units for use in Standard Controls from Safety CPU Units.
Standard Programmable Controller (Standard PLC)	A Programmable Controller (PLC) that is used for Standard Controls. “Standard PLC” is used to distinguish a PLC for Standard Controls from a PLC for Safety Controls.

Acronyms

Acronym	Meaning
CIP	Common Industrial Protocol
EPI	Expected Packet Interval
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PPS	Packets Per Second
RPI	Requested Packet Interval
TUNID	Target Unique Network Identifier

Index

A

ABORT, 68
abort errors, 496
ABORT Mode, 68
access control, 158
access password, 158
access password for user-defined function blocks, 159
activation key, 159
Activation Key Dialog Box, 398
adding an input assembly, 261
adding an output assembly, 262
adding connections, 251
adding devices to a network, 246, 289
adding objects to the library, 397
adjusting EPI, 185
adjusting RPI, 185
Advanced Connection Settings Dialog Box, 256
Advanced Setup Button, 256
alarm, 472
allowed Unit communications bandwidth, 186
alternate DNS server, 99
arranging function blocks, 378
arranging text boxes, 383
assembly data, 121
Auto Allocation, 251
automatic connection setting, 272
automatic operation, 453
automatic operation at startup, 453
automatic recovery, 136
automatic refreshing of device status display, 471
automatically registering and unregistering connections, 254

B

Backplane, 232, 284
bandwidth, 186
bandwidth usage, 321
bandwidth use rate, 319
baud rate, 99
baud rate DIP switch, 48
Bit strobe, 109
BOOTP, 288
BOOTP client, 98
boots, 419
Build, 389

C

Calculate EPI Button, 313
Calculate EPI Dialog Box, 313, 318
calculated PDF values, 545
calculated PFH values, 545
calculating communications response performance, 183
calculating response performance, 183
calculating system performance, 170
centralized control, 22
Change Device Comment, 234, 248, 290
Change Device Settings Dialog Box, 318
Change IP Address, 290
Change Mode, 445
changing device addresses, 247, 289
changing I/O assemblies, 262
changing the communications cycle time for Standard I/O Communications, 318
changing the connected network, 431
changing the device mode, 445
changing the device name, 234, 248, 290
changing the EPI, 322
changing the EPI for each Safety Connection, 315
changing the EPI settings, 184
changing the mode, 236
changing the network, 431
changing the operating mode, 164, 461
changing the password, 215
channel mode, 141, 152
channel mode for Safety Output terminals, 152
chattering, 150
checking and adjusting the system response performance, 191
checking cycle times, 181
checking network bandwidth usage, 183
checking programs for syntax errors, 389
checking the communications response performance, 313, 320
checking the NE2A-series Controller cycle time, 311
checking the network reaction time, 189
checking the version, 208
clearing the error history, 476

communications cycle time, 109
communications cycle time settings, 183
Communications Cycle Time Tab, 484
communications specifications, 93
Communications Unit tab page, 242
configuration lock, 194
CONFIGURATION Mode, 68
CONFIGURATION RESTORE Mode, 68
connecting input devices, 143
connecting input/output signals, 382
connecting to a network, 425
connection, 102, 382
connection information, 104
connection specifications, 93
connection type, 104
connectors (modular plug), 419
COS, 109
CPU Unit, 35
CPU Unit errors, 496
Create from I/O Tag List Dialog Box, 369
creating new variables, 265
creating program objects, 397
creating program projects, 364
creating programs, 376
creating sections, 385
creating the configuration restore file, 456
creating user-defined function blocks, 394
creating variables, 79, 366
critical errors, 496
CRITICAL FAULT Mode, 68
Cross Reference Window, 391
current sourcing, 60
cycle time, 181, 236
Cyclic, 109

D

D40A, 145
D40A Non-contact Switch, 145
data after communications error, 136
default gateway, 99
delay time, 187
delay time in Tag Data Links, 187
deleting a device, 248, 290
deleting connections, 252
deleting I/O assemblies, 262
detail codes, 495
device information, 110
device menu, 225
device password, 158, 447
device properties, 442
device status, 470
DeviceNet communications, 95
DeviceNet connector, 49
DeviceNet I/F, 426
DeviceNet Interface Board, 426
DeviceNet network setting procedure, 240
DeviceNet network settings, 245
DeviceNet Safety communications, 102
DeviceNet Safety Unit, 46
DeviceNet Standard Communications, 107
DeviceNet Unit errors, 509
devices with mechanical contact outputs, 59
devices with PNP semiconductor outputs, 60
dimensions, 34, 40
DIP switch, 37
discrepancy error, 149, 150
Discrepancy Time, 340
discrepancy time, 148
distributed control, 22
DNS server, 99
domain name, 99
downloading, 432
downloading device parameters, 432
downloading parameters, 161, 458
dual channel complementary, 348
dual channel equivalent, 149, 348
Dual Channel Mode setting, 154

E

Edit All Connections Dialog Box, 256
Edit Connection Dialog Box, 251, 253, 254
Edit Device Parameters Dialog Box, 249, 260, 273
Edit I/O Comments Dialog Box, 339
Edit Local Input Terminal Dialog Box, 347
Edit Local Output Terminal Dialog Box, 343
edit menu, 223
Edit Safety Target I/O Dialog Box, 263
Edit Target I/O (EtherNet/IP) Dialog Box, 301

editing all connections, 256
editing bit comments, 266, 304, 368
editing connections, 253
EDS file menu, 226
End Cover, 41
End Unit, 42
EPI, 105, 189, 255, 313
EPI calculation, 184
error category, 496
error codes, 495
error connection, 136
error detection during self-diagnosis, 150, 154
Error Device List Dialog Box, 435
error handling, 150, 154
Error History Tab, 484, 487
error latch time, 151, 155
error status, 125, 126
errors during downloading, 435
Ethernet connector, 55
Ethernet I/F, 428
Ethernet Information Tab, 489
Ethernet Switching Hub, 101, 137
Ethernet switching hub functions, 187
EtherNet Unit errors, 522
Ethernet wiring, 419
EtherNet/IP communications, 97
EtherNet/IP network setting procedure, 282
EtherNet/IP Safety Communications, 111
EtherNet/IP Safety Unit, 51
EtherNet/IP Standard Communications, 113
execution delay, 75
Expected Packet Interval, 105
exporting, 83
exporting variables, 371
Extend Mode, 236
Extend Mode Tab, 456

F

Fault Present, 126
file menu, 222
finding a variable, 373
Force Mode, 71, 466
force-setting and force-resetting, 71
force-setting/resetting, 466
forgotten passwords, 159
function block settings, 379
function blocks, 84, 88

G

general precautions, xx
general status, 124
Get from the actual network Button, 233, 246
glossary, 547
GMRP, 137

H

Hardware List Pane, 218
help menu, 228
Hide busy variables Check Box, 391
host ID, 287

I

I/O assembly, 255
I/O assembly name, 263
I/O connections, 255
I/O specifications, 58, 63
I/O Tag List Window, 369
I/O tags, 77, 377
I/O terminals, 59
I/O Unit Tab Page, 333, 342
ID allocation, 105
IDLE, 68
Idle, 236
IDLE Mode, 68
IGMP client, 98
IGMP snooping, 137
Import, 217, 400
Import Network Configuration Dialog Box, 217
importing, 83
importing NE1A-series programs, 400
importing NE1A-series user-defined function blocks, 400
importing user-defined function blocks, 396
importing variables, 372
indicators, 35
INITIALIZING, 68
INITIALIZING Mode, 68

Input Bits Dialog Box, 339
input channel mode, 141
inspections, 542
installation direction, 409
installation in control panel, 408
installation position, 408
installing, 195
instruction execution cycle time, 181, 311
internal variables, 381
IP address, 98
IP address display, 53
IP address switch, 54

L

laws and regulations, xxi
library folder, 397
list of data that can be registered, 263
list of registered devices, 250
local I/O, 78
lock mark, 452
locking, 162
locking the configuration, 162, 459
locking the device configuration, 451
Logic Editor, 353
Logic Editor menus, 355
lost device passwords, 448

M

Maintenance Mode, 220, 470
managing operation, 30
manual connection setting, 272
Master Function Status Area, 481, 483
MAT, 146
maximum I/O response time, 177, 179
Memory Card DIP switch, 37
Memory Card functions, 37
Memory Card models, 39
menu commands, 222
Message Report Pane, 218
minimum I/O response time, 178, 180
mismatching parameters, 441
mode change, 69
modification password, 158
modification password for user-defined function blocks, 159
monitoring, 464
monitoring device status, 471
monitoring DeviceNet Units, 480
monitoring EtherNet/IP Units, 486
monitoring local I/O status, 477
monitoring programs, 464
monitoring Safety Connections, 474
monitoring the error history, 475
monitoring the operation log, 478
mounting Communications Unit, 412
mounting End Plates, 413
mounting I/O Units, 411
mounting the DIN Track, 413
moving between operating modes, 69
moving function blocks, 378
multicast, 104
multicast connection, 93, 104, 115
multicast filtering, 137

N

NE2A Backplane, 232
NE2A USB Port, 425
NE2A_Backplane, 232
NE2A-series Backplane, 284
network bandwidth, 183
network bandwidth usage, 183
Network Configuration List, 221
Network Configuration Pane, 218
Network Configurator errors, 530
network delay, 105
network download, 433
network ID, 287
network menu, 224
network number settings, 233
network numbers, 95
Network Property Dialog Box, 233, 245
network reaction time, 173, 313, 320
Network Status Area, 487
network system configuration, 92
network upload, 437
New User Function Block Dialog Box, 394
New Variable Dialog Box, 303
node address, 97

node address duplication error, 97
node address switch, 48
non-fatal errors, 496
non-safety data, 107, 115
normal status, 126
Not Used, 141, 152
number of local I/O points, 140

O

online connection, 425
online monitoring, 464
open type, 104
operating modes, 68
operation and maintenance using a Memory Card, 161
operation rights for user-defined function blocks, 394
option menu, 227
Output Bits Dialog Box, 337
output terminals, 64
output variables, 381

P

page setup, 404
parameter protection, 236
password, 158
password for network configuration files, 214
password protection for network configuration files, 214
periodic inspection points, 542
peripheral servicing cycle time, 181, 311
point-to-point connection, 115
Poll, 109
power supply terminal block, 39
Power Supply Unit, 43
precautions when selecting a switching hub, 137
preferred DNS server, 99
print preview, 403
printer settings, 404
printing, 402
program execution delay, 75
program execution delay time, 236
program size, 85
Program Window, 465
project file, 398
project file password, 158
Protection Mode, 216

Q

QoS, 137
Quality of Service, 137

R

reaction time, 171, 189
reaction time calculation, 172
reading network configuration files, 212
Register Device List Area, 251
Register to Routing Network, 242, 243, 284
Register/Unregister Button, 254
registering data, 264, 302
registering DeviceNet Units, 241
registering EtherNet/IP Units, 283
registering I/O assemblies, 305
registering I/O assemblies for Safety Slaves, 259
registering I/O assemblies for Standard Slaves, 273
registering I/O assemblies from the Logic Editor, 267
registering Safety Slaves, 249, 292
registering Standard Slaves, 269
registering the CPU Unit, 234
regulations, xxvi
remote I/O, 78
remote I/O allocation, 121
Remote Safety I/O area, 135
Remote Standard I/O related data, 127
removing a Communications Unit, 415
removing an I/O Unit, 413
replacing a variable, 374
Requested Packet Interval, 119
reset types, 455
resetting, 73, 454
resetting a device, 454
resetting DeviceNet Unit, 73
resetting errors, 151, 155
resetting EtherNet/IP Unit, 74
response performance, 26, 177, 178
response performance of DeviceNet Standard I/O Communications, 177
response performance of EtherNet/IP Tag Data Link communications, 178
response performance of Standard Communications, 177

RESTART, 39
restart, 73
restarting, 164
restarting operation, 461
restore default settings and then restart, 73
restore default settings except for specified variables and then restart, 73
Restore Operation Mode, 236
restore operation setting, 457
reusing programming, 398
Router Devices, 222
routing, 101
RPI, 119, 320
RPIs of Tag Data Link Connection, 324
RUN, 38, 68
RUN Mode, 68, 453
Run/Idle Operation Mode, 236
RUN/IDLE operation setting, 457
RUN/STOP/RESTART switch, 38, 164, 461

S

Safety, 152
safety chain, 171
safety connection communications reopen switch, 127
safety connection error status, 126
safety connection normal status, 126
Safety Connections, 102, 111
Safety Connections Tab Page, 250
safety control, 24
Safety CPU Unit, 35
safety data, 107, 115
safety device with a contact output, 143
safety device with a semiconductor output, 147
safety I/O bits, 336
Safety I/O Information Tab Page, 443
Safety Input, 141
Safety Input Unit, 57
safety inputs, 58
safety mark, 440, 452
Safety Mat, 146
Safety Network Controller, 2
Safety Output Unit, 62
safety outputs, 63
safety precautions, xxii
Safety Pulse Test, 152
safety signature, 104
Safety Slave I/O Tab Page, 261
saving network configuration files, 210
saving the error history, 476
searching for function blocks, 389
searching for unconnected function blocks., 389
Searching for Variables in the Program, 391
Select Network Dialog Box, 243
selecting networks, 21
SERVICE switch, 38
Set Packet Interval (RPI) Dialog Box, 185, 321, 325
setting a Dual Channel Mode, 147
setting assembly data, 263, 276, 296
setting device parameters, 235
setting I/O assemblies, 300
setting IP addresses, 286
setting NE2A-series operation at startup, 75
setting network numbers, 245
setting parameters for local I/O, 332
setting Safety Connection parameters, 254, 294
setting safety input bits, 345
setting safety output bits, 342
setting Slave input data in IDLE Mode, 277, 306
setting Standard Connections, 271
setting TCP/IP, 98
setting the Channel Mode, 343, 346
setting the operating mode after a communications error, 136
setting the parameters for safety I/O bits, 336
Setup TCP/IP Configuration Dialog Box, 291
seven-segment display, 37, 494
Signature Tab Page, 444
single cast connection, 104
Single-beam Safety Sensor, 144
Slave Function Status Area, 481, 483
Slave I/O (DeviceNet) Tab Page, 273
specifications, 33
Standard Connection, 108
standard control, 24
Standard I/O Communications cycle time, 313
Standard I/O Communications cycle time settings, 183
Standard Master, 278
standards, xx, xxvi
starting, 164

starting and stopping execution of all NE_A-series Controllers, 165
starting program execution, 461
starting the Network Configurator, 207
status bar, 228
status related data, 124
Status Tab, 480, 486
STOP, 38
stopping, 164
stopping or restarting communications after an error, 258
stopping program execution, 461
subnet mask, 99
switches, 37, 48, 54
switching hub, 100, 419
switching hub functionality, 137
switching hub types, 137
system configuration, 9
system performance verification, 308
system requirements, 194

T

table of security functions, 166
Tag Data Link communications, 113
Tag Data Link connections, 114
Tag Data Links and specifications, 97
Target/Slave I/O Settings Dialog Box, 267
TCP/IP Settings Dialog Box, 287
terminal layout, 57, 62
test inputs, 58
Test Output Mode, 142
Test pulse from test output, 141
test pulse, 344
Test Source, 340
time out multiplier, 105
tool menu, 227
troubleshooting, 491
TUNID, 95
twisted-pair cable, 419
types of variables, 76

U

uninstalling the Network Configurator, 196
unit number rotary switch, 48, 54
unit replacement, 543
Unit Status Area, 487
Unit Status Tab, 482
Unlock, 452
unlocking the device configuration, 452
unregistering data, 265, 302
Update Device Configuration Dialog Box, 315
updating the error history, 476
uploading, 436
uploading device parameters, 436
Usage of Device Bandwidth, 320
Usage of Network Bandwidth, 313
USB port, 39, 425
Used as Safety Input, 141
user program ID, 236
user-defined function block file, 398
user-defined function blocks, 380
using the NE2A-series Controller as a Safety Slave, 259, 296
using the shortcut keys in the Logic Editor, 361

V

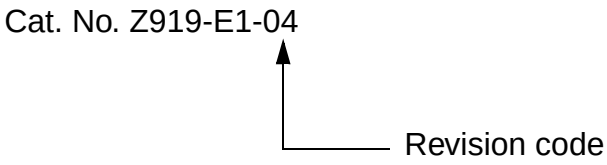
validating the configuration restore file, 458
variable data files, 83
Variable Reference Report Window, 390
variable specifications, 80
verification, 439
verifying device parameters, 439
verifying parameters, 439
view menu, 224

W

warning, 472
watching, 464
watching variables, 464
welding check, 337
wiring, 416
wiring output devices, 153

Revision History

A manual revision code appears as a suffix to the catalog number on lower left corners of the front and back covers of the manual.



The following table outlines the changes made to the manual during each revision. Page numbers refer to the previous version.

Revision code	Date	Revised content
01	March 2009	Original production
02	December 2009	Corrected mistakes.
03	January 2010	Corrected mistakes.
04	May 2011	Made changes for new version of the Network Configurator, made changes and additions for applicable OS specifications, and added descriptions of new functions.

OMRON Corporation **Industrial Automation Company**
Tokyo, JAPAN

Contact: www.ia.omron.com

Regional Headquarters
OMRON EUROPE B.V.
Wegalaan 67-69-2132 JD Hoofddorp
The Netherlands
Tel: (31)2356-81-300/Fax: (31)2356-81-388

OMRON SCIENTIFIC TECHNOLOGIES INC.
6550 Dumbarton Circle,
Fremont, CA 94555-3605 U.S.A.
Tel: (1) 510-608-3400/Fax: (1) 510-744-1442

OMRON ASIA PACIFIC PTE. LTD.
No. 438A Alexandra Road # 05-05/08 (Lobby 2),
Alexandra Technopark,
Singapore 119967
Tel: (65) 6835-3011/Fax: (65) 6835-2711

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-5037-2222/Fax: (86) 21-5037-2200

Authorized Distributor:

© OMRON Corporation 2009 All Rights Reserved.
In the interest of product improvement,
specifications are subject to change without notice.

Printed in Japan
Cat. No. Z919-E1-04 0511